

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
12 September 2003 (12.09.2003)

PCT

(10) International Publication Number
WO 03/075570 A1(51) International Patent Classification⁷: H04N 7/16, 7/167

(21) International Application Number: PCT/PL03/00013

(22) International Filing Date: 20 February 2003 (20.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data: *06 Sp 04*
 P-352643 6 March 2002 (06.03.2002) PL
 P-354371 10 June 2002 (10.06.2002) PL

(71) Applicants (for all designated States except US): **ADVANCED DIGITAL BROADCAST POLSKA SP. Z O.O.** [PL/PL]; ul. Trasa Polnocna 16, 65-119 Zielona Gora (PL). **ADVANCED DIGITAL BROADCAST LTD.** [—/—]; 8/F, 145 Chung Shan North Road, Section 2, Taipei 104 (TW).

(72) Inventors; and

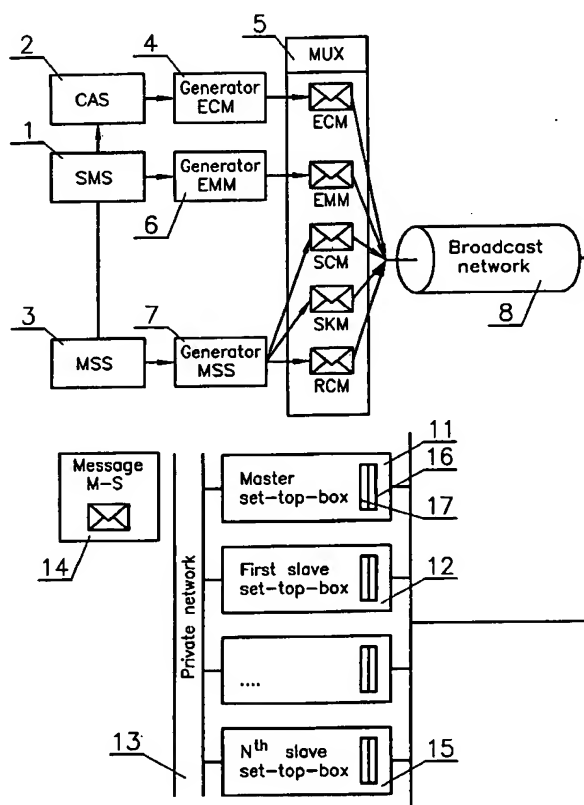
(75) Inventors/Applicants (for US only): **DOGANOWSKI, Wojciech** [PL/PL]; ul. Wegierska 3/7, 65-001 Zielona Gora (PL). **CHEN, Sin, Yi** [—/—]; 15 Lane 29, Ta-Shei Street, Hsin Tien, Taipei 111 Taiwan (TW). **HEMPHILL, Earl, Stanley** [US/—]; 32, Lane 16, Section 1, Chung Cheng Road, Taipei 111 Taiwan (TW). **PAWLOWSKI, Adam** [PL/PL]; ul. Rajdowa 14 m.85, 94-003 Lodz (PL).

(74) Agent: **HUDY, Ludwik**; Czernichów 4, PL-32-070 Czernichów, Kraków (PL).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: BROADCAST NETWORK ACCESS-MANAGEMENT SYSTEM AND METHOD FOR MANAGEMENT OF RECEIVERS OPERATING WITHIN BROADCAST NETWORK



(57) Abstract: In a broadcast network access-management system comprising at least one master decoding device provided with a smart card, and at least one slave decoding device linked to it, and a transmitter device which generates and transmits entitlement management messages intended for the linked master and slave decoding devices and other devices, the master decoding device (11) and at least one slave decoding device (12) linked together are located in a defined distance and operate when a distance between them does not exceed the defined distance dependant upon a cable length, a configuration, a number and quality of splitters and connections.

WO 03/075570 A1



(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*
- *of inventorship (Rule 4.17(iv)) for US only*

Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

BROADCAST NETWORK ACCESS-MANAGEMENT SYSTEM AND METHOD FOR MANAGEMENT OF RECEIVERS OPERATING WITHIN BROADCAST NETWORK

TECHNICAL FIELD

The invention relates to a management system of access to a television broadcast network and a method for management of receivers operating within this network.

BACKGROUND ART

A management system of access to a broadcast network is known from the US Patent No. 5,748,732 which describes a management system of access to a network and a device verifying access to a network which comprises slave set-top boxes and a master set-top box controlling access to the network. The master set-top box receives slave entitlement information from a central management device and writes the slave entitlement messages to smart slave cards when the latter are inserted in the master set-top box and then read in the slave set-top box.

AIM OF THE INVENTION

The invention seeks to provide a management system which can prevent unauthorised transfer of the secondary and further decoding devices, referred to as slave decoding devices, beyond permitted and defined limits within the network.

DISCLOSURE OF THE INVENTION

The object of the invention is a broadcast network access-management system comprising at least one master decoding device provided with a smart card, and at least one slave decoding device linked to it, and a transmitter device which generates and transmits entitlement management messages

intended for the linked master and slave decoding devices and other devices. The master decoding device and at least one slave decoding device linked together are located in a defined distance and operate when a distance between them does not exceed the defined distance dependant upon a cable length, a configuration, a number and a quality of splitters and connections.

Preferably a decoding device is assigned the status of the master decoding device only after it has been linked to a network and an entitlement control message for the master decoding device has been found.

Preferably the master decoding device imposes on the transmitter device a transmission of the entitlement control message appropriate for the master decoding device.

Preferably a decoding device is granted with a mode of the slave decoding device only after it has been linked to a network and an entitlement control message for the slave decoding device has been found.

Preferably the slave decoding device imposes on the transmitter device a transmission of the entitlement control message appropriate for the slave decoding device.

Preferably the master decoding device and the slave decoding device, when they are turned on, first check if any messages are being transmitted by other devices before they start to transmit messages.

Preferably the slave decoding device triggers the master decoding device to transmit the entitlement control message appropriate for the slave decoding device and messages with demand for coupling.

Preferably a period of time for coupling the master decoding device with the slave decoding device is pre-set.

Preferably the slave decoding device is provided with a microprocessor card.

Preferably the defined distance between the master decoding device and the slave decoding device linked to it is determined from the level of a signal exchanged between the master decoding device and the slave decoding device.

Preferably the level of the signal exchanged between the master decoding device and the slave decoding device is compared with the level of the signal sent between them during preceding communication.

Preferably decoding devices are assigned the status of the master decoding device and the slave decoding device after transmission of encoded messages by the transmitter device generating and transmitting specified codes.

Preferably a private television network shares physical linkages with a broadcast network.

Preferably the entitlement management messages, allowing the master decoding device and at least one slave decoding device an access to the broadcast network, are transmitted after the encoded messages are sent by the transmitter device which is designed to generate and transmit specific codes.

Preferably management messages sent to the master and the slave decoding devices are generated by a generator connected to a multiplexer through another generator which creates messages, and the management messages sent to the master and the slave decoding devices are included in the entitlement management message.

Preferably messages exchanged between the master decoding device and the slave decoding devices are messages used to identify the master decoding device and the slave decoding devices, systems that are their component parts, or external devices linked to them.

Preferably the identifying messages include a type of the master decoding device and the slave decoding devices, their version and/or their serial number.

Preferably messages exchanged between the master decoding device and the slave decoding devices are messages used to identify software.

Preferably the messages used to identify software include a version number and/or a serial number of the software.

Preferably messages exchanged between the master decoding device and the slave decoding devices are messages facilitating interaction between

the decoding devices, systems integral to them, or between software installed in the decoding devices or devices co-operating with them.

Preferably messages exchanged between the master decoding device and the slave decoding devices are messages which incorporate an operating status of a given device/program, a result of a certain operation, an order to execute a certain operation and data collected or processed by a certain device/software.

Preferably messages exchanged between the master decoding device and the slave decoding devices are messages generated either within the decoding devices or delivered from external sources.

Preferably messages exchanged between the master decoding device and the slave decoding devices can be internet data, text messages, streams and files containing sound, pictures, video and software, and/or updates of software.

Preferably messages exchanged between the master decoding device and the slave decoding devices can contain additional messages generated by software installed in the decoding device or devices which are co-operating with them, or messages which are delivered to the decoding devices from outside sources.

Preferably messages exchanged between the master decoding device, the slave decoding devices, and outside devices consist of synchronising bytes, a heading with a source and a destination addresses, a type of message, a flag with information as to whether the message contains data and the size of the block of data, and also data constituting the message (referred to as a payload), and a checksum.

The object of the invention is also a management method of receivers provided with smart cards and linked to a television broadcast network, among which at least one device is the master decoding device with at least one slave decoding device linked to it and an interlinked transmitter device which generates and transmits messages that allow to use the master and the slave decoding devices and receivers connected to them. In such an arrangement the master decoding device and at least one linked slave decoding device are

installed at a defined distance from each other so that the master decoding device and the slave decoding device will operate only if the distance between them does not exceed the defined nominal distance dependant upon the number, the configuration, and the quality of splitters and links.

BRIEF DESCRIPTION OF DRAWINGS

The object of this invention is shown in implementation examples in the enclosed drawings, in which:

Fig. 1 illustrates a block scheme of system management;

Figs 2, 3, 4, and 5 illustrate block schemes of a master and slave set-top boxes interconnections;

Figs 6A and 6B illustrate a flow diagram of an algorithm of set-up process of set-top boxes;

Figs 7A and 7B illustrate a flow diagram of an algorithm of operation of a slave set-top box;

Figs 8A, 8B, 8C and 8D illustrate a flow diagram of an algorithm of operation of a master set-top box;

Figs 9A, 9B, and 9C illustrate a flow diagram of an algorithm of sending a ping message;

Fig. 10 illustrates a flow diagram of an algorithm-governed process of sending messages;

Figs 11A and 11B illustrate states of set-top boxes within the broadcast network;

Fig. 12 illustrates a system comprising set-top boxes where a method of sending messages between two set-top boxes is presented;

Fig. 13 illustrates a system comprising set-top boxes where a method of sending messages between the set-top box and an external device is presented;

Fig. 14 illustrates a structure of a message sent between two set-top boxes;

Fig. 15 illustrates a flow diagram of message preparation procedure;

Fig. 16 illustrates a flow diagram of the procedure of receiving message.

BEST MODE FOR CARRYING OUT THE INVENTION

The television network system presented in fig. 1 comprises a Subscriber Management System 1, (SMS), which stores information about clients and assigned smart cards, and which is connected with a Conditional Access System 2, (CAS), and with a management system of decoders, in invention description referred to as set-top boxes or decoding devices, called a Master Slave System 3, (MSS). The Conditional Access System 2 through a generator 4 generating Entitlement Control Messages, (ECM), sends messages to a multiplexer 5 which multiplexes different data streams into one integrated stream of data. The multiplexer 5 receives also messages from a generator 6 creating Entitlement Management Messages, (EMM), messages from a generator 7 that generates set-top box management messages which are messages allowing coupling between master and slave set-top boxes, so-called Set Coupling Messages, (SCM), messages concerning the master set-top box verifying key, called Session Key Messages, (SKM), and messages used to reset the coupling of the master and the slave, called Reset Coupling Messages, (RCM).

The ECMs are messages used to decrypt the stream of data, and contain a symmetrical private key, which is used both by the transmitting and the receiving device. The ECMs are encrypted with the use of an asymmetrical key. The private part of the asymmetrical key resides in the transmitting device and the public part of the asymmetrical key is sent in the EMM. The latter contain information necessary for decoding ECMs, which means that these messages are controlling the access to the data stream. The EMMs are controlling the access to the ECMs.

The integrated stream of data from the multiplexer 5 is sent, over a broadcast network 8, to the master set-top box 11 and the slave set-top boxes 12 and 15, which are provided with a device 16 for coding and reading smart cards 17. The master set-top box 11 and the slave set-top box 12 are additionally linked through a private television network 13, within which, after the set-top boxes have been coupled, various messages 14, called Master

Slave Messages, (MSM), are sent. In particular solutions, the private television network 13 can share the physical medium with the broadcast network 8. In the case of the shared medium, elements of the broadcast network 8, i.e. cables, splitters, are used, for example, to pass coupling messages for the master set-top box 11 and the slave set-top box 12.

Figs 2, 3, 4, and 5 illustrate different configurations of links between the set-top boxes through the private network 13 shown in fig.1. A cable 185, shown in fig. 2, led to a building, has a two-way splitter 184 from which cables are led to the next two-way splitters 183, 186 in different apartments. In one of these, there are the master set-top box 182 and the slave set-top box 181 whilst the master set-top box 188 and the slave set-top box 187 assembly is located in the second apartment. In each apartment, set-top boxes can be placed in different rooms.

In another arrangement the cable 195, shown in fig. 3, is led to the building and is terminated with a two-way splitter 194 from which cables are led to a second two-way splitter 196 and a four-way splitter 193 located in different apartments. In one of these apartments, there are the master set-top box 192 and three slave set-top boxes 191, 197, 198, while the master set-top box 200 and one slave set-top box 199 are located in the second apartment.

In another possible arrangement the cable 201, shown in fig. 4, is led to the building and is provided with a four-way splitter 212 from which cables are led to further four-way splitters 202, 207 located in two different apartments. In one of these apartments, there are the master set-top box 203 and three slave set-top boxes 204, 205, 206. In the second apartment the identical system is installed: the master set-top box 208 and three slave set-top boxes 209, 210, 211.

In the final layout, the cable 225, shown in fig. 5, is led to the building and has a four-way splitter 224 from which one cable is linked to a two-way splitter 223 with the master set-top box 226 and the slave set-top box 227 connected in one apartment but in two different rooms. The second cable from the splitter 224 is led to a four-way splitter 221 in a second apartment where

the master set-top box 222 and three slave set-top boxes 228, 229, 230 are linked.

Each of the set-top boxes, shown in figs 2, 3, 4, and 5, operates at a specified location within the broadcast network. Each slave set-top box is interrelated with the defined master set-top box and can not change its position without modification of the settings. It means that the set-top box can not be moved beyond limits defined by a cable length, a configuration, a number and a quality of splitters between these two set-top boxes. A change of position, followed by a change of link configuration, results in changes of the signal level passing from a set-top box to a set-top box as a consequence of the modification of the connections and the change in the resistance of the cables linking the set-top boxes. To detect changes in the set-top box location in the present solution, a minimal signal level, necessary to make the connection between the master set-top box and the slave set-top box possible, depending on the location of the slave set-top box within the network, is used. This signal level is very specific for each set-top box and allows for a logical calculation of a maximum operating distance between the set-top boxes to be made. In the case of broadcast and private networks, the cable connecting the set-top boxes, as well as the electrical characteristics of the splitters, are used in the estimation of the distance between the master and the slave set-top boxes. This distance is defined as producing a minimum signal level necessary to pass a message from the master to the slave set-top box or vice-versa. The master and the slave set-top boxes memorise the minimum signal level used during the previous communication and compare it with the signal level during the next operation or while checking the stability of the configuration. If the difference in the signal level is greater than a permissible value with a certain margin, an error message will be sent, and a proper action will be taken, assuming that if the network has not been modified, the environment should not change within a short period of time. In the suggested solution, a particular set-top box should be able to modify a signal level within at least a 50 dB range in one decibel increments.

The subscriber management system, including the set-top box management system, is software operated, and specific algorithms assigned to different types of set-top boxes and functions are presented in the next figures.

Figs 6A and 6B illustrate an algorithm of a set-up process of set-top boxes. When a set-top box starts to operate, the mode of operation and the status of the set-top box, initially unknown (the new set-top box should work in a neutral mode and then attempt to determine its role) as it is stated in table 23, are restored in step 22. Later on, in step 24, the mode of the set-top box is verified in attempt to determine its master or slave role. At the same time it is checked whether any disconnection occurred between the master and the slave set-top boxes during the last communication. In case of occurrence of such a disconnection, video display is disabled in step 25. Should the opposite case pertain, the state of the set-top box is verified in step 26, and if it is still unknown, the status of the set-top box is initialised in step 27. Then, messages relating to coupling between the master set-top box and the slave set-top box are searched for in step 28. If they are not found in step 29, and the session time has elapsed in step 30, after waiting 10 seconds in step 31, a new attempt to find the entitlement control message is performed. Once entitlement control messages and set coupling messages between the master set-top box and the slave set-top box are found, they are sent to the smart card in step 32 and next it is verified in step 33 if the set-top boxes are authorised for these coupling messages. In the case of a positive answer, the operating mode of the master set-top box is granted to the set-top box in step 34. In the case of a negative answer, in step 35, the operating mode of the slave set-top box is granted to the set-top box and the set-top box is assigned an inactive status, and in both cases the system resumes operation.

If the mode of the set-top box is recognised as known, in step 40 the demultiplexer is set to send SKMs and RCMs. When it is determined in step 41 that the set-top box operates in the master mode, in step 42 the demultiplexer is set to send SCMs and the set-top box is ordered to operate in the master mode in step 43. If the set-top box is not recognised as the master it is ordered in step 44 to work in the slave mode. Messages, obtained from the

demultiplexer after waiting for a certain period in step 45, are verified in step 46. After the set coupling messages are received, the set-top boxes are coupled in step 47 and the data of the slave set-top box are stored. If SKMs were received, in step 48, the data relating to the session in progress are stored in step 49. In the case when the RCMs are received, in step 50, the set-top box is deleted from a slave set-top box list, the SKM is removed and the mode of the set-top box is set as unknown in step 51, and finally the set-top box is disabled in step 52, and the system operation is resumed.

Figs. 7A and 7B illustrate an algorithm of operation of the slave set-top box, which, when turned on, waits in step 62 for a message from the master set-top box to establish coupling. A call for coupling can be repeated when a coupling order is received. If the set coupling message is positively verified in step 64, then it is further verified in step 65 to find whether this message allows video to be displayed. For the coupled slave set-top box, for which the coupling time has expired, which is checked in step 67, the video is again enabled in step 66. The non-coupled set-top box is set as the coupled one in step 68, and a repetition of the process is followed.

If the received set coupling messages are not correct, it is checked in step 70, whether the set-top box is already coupled or whether it is the first coupling. A negative answer is followed by a verification whether the set-top box is in the state of coupling or is already coupled in step 71, and if not, the coupling process is repeated. If the coupling time of the non-coupled set-top box does not exceed the time allowed for coupling, which is verified in step 72, in step 73 a message with a call for coupling is sent. The verification of the time assigned to display video takes place in step 74, and if this time has expired, in step 76, a message calling for coupling is sent. Then, in step 75 the time assigned to display video is verified, and if it has expired, in step 77 the status of the set-top box is changed to the time-expired status, followed by disabling video in step 78, next an error message is sent in step 79, and a coupling repetition takes place.

Figs 8A, 8B, 6C and 8D illustrate an algorithm of operation of the independent, or the master set-top box, which, when turned on, waits in step 82

for a message which is verified in step 83. Then, in step 84, it is checked whether the status of the master set-top box meets requirements of the coupling process. If the status of the master set-top box does not suit the coupling instruction, it returns to the waiting status. Subsequently, a check is made in step 87 as to whether the message is a request for coupling. A negative answer is followed by the return to the waiting status, whereas if the verification brings confirmation, a probing message is sent in step 89. In step 90 the status is examined, which should be the status of coupling with the slave set-top box. If so, in step 91 a threshold signal level is stored and the status of the slave set-top box coupled is allotted, followed by a message sent in step 92 to the coupled slave set-top box to enable video. The signal level is checked in step 93, and if it differs from the signal more than a permissible margin, the slave set-top box in step 94 is granted with a status of being disconnected, an error message is sent in step 95, and the master set-top box is returned to the waiting status. In step 97 a verification is carried out to decide if the time assigned for coupling has elapsed, and then in step 98 if the operating time has expired. Beginning from step 99, in steps 100, 101, and 102 the mode of each active set-top box is compared with the mode of the slave and connected set-top box, a verification process ends with a message sent to enable video display, whereas from step 103 the master set-top box is returned to the waiting status.

In case of a timeout of the master set-top box, in step 104, the verification process of each active slave set-top box is carried out, beginning with a probing message sent to the first slave set-top box in step 105, and then in step 106 a signal level is compared to a certain set level. The process of verification of the first active slave set-top box ends in step 111 and is carried starting with each next slave set-top box. If the difference in the signal level is not greater than an allowed margin, a new threshold signal level is stored in step 107, and in step 108 information to enable video display is sent. If the signal differs by more than the allowed margin, in step 109 the slave set-top box is granted with the status of non-connected, and an error message is sent in step 110.

Figs 9A, 9B, and 9C illustrate an algorithm of sending a ping message to a chosen location within a network. First, in step 116 the following parameters are established: the maximum and constant number of steps, the maximum signal level which equals two raised to the power of the maximum step number, the signal power equal to half of the maximum signal power, the robustness having a constant value, and the step which equals unity. Next, a coupling message is sent in step 117 and receiving of message confirming the coupling takes place in step 118. In step 119 the time predicted to receive an answer to the ping message is verified. Calls for ping message repetitions are transmitted in step 114. If the waiting time predicted to receive confirmation of coupling is exceeded, in step 132 it is checked whether the robustness is greater than zero, and in step 133 whether the step number is less than the maximum number of steps. For a negative answer the signal power is stored in step 134 and the process of sending the ping message ends in step 135. In step 136 the step number is increased, the signal power is established as equal to the maximum power divided by two raised to the number of incremental power steps, the initial robustness is set, followed by the repetition of sending the ping message. If the number of steps is less than the maximum number of steps, which is verified in step 140, the number of steps is increased in step 143, in step 144 the signal power is established as being equal to two raised to the number of incremental power steps, the initial robustness is set, followed by the repetition of sending the ping message. The robustness, set in step 144, is a parameter used to establish the number of probing operations which take place until communication is recognised as unsuccessful. For a step number not less than the maximum step number, the signal level is recorded in step 141 and the process of sending the ping message ends in step 142.

Fig. 10 illustrates an algorithm-governed process of sending messages, which after start is followed by zeroing the N number in step 121. In step 122 the set-top box waits for silence in the network. A set-top box, which does not need to transmit data, initially checks if any other set-top box has started sending messages to it. Similarly, if the set-top box has messages to transmit, it listens within the network for signals transmitted from the other set-top box,

which means that the former is tuned to a carrier, and messages are sent only if no other signal is detected and the private network is idle. In step 123 a message is sent, in step 124 a message is received. In step 125 it is verified whether one of received messages is a confirmation to the message sent earlier. If there is no collision, i.e. messages sent and received are the same, the algorithm ends in step 126. In case of collision occurring (in the event of the messages not being equal), in step 127 the number N is increased followed by waiting in step 128 by a random waiting time and the process is repeated. A formula to calculate the period of waiting is described in table 129.

Figs. 11A and 11B illustrate states of set-top boxes within the broadcast network. At the moment of start, the mode and the status of each set-top box is not predetermined, which implies that the current mode and status are unknown. When the set-top boxes 174, 175, 176, 177, 178, 179, being in any state, receive a RCM 281, they change their state 172 to unknown. A set-top box being in unknown 172 state always sets itself into the undetermined 174 mode and initialises its operation. The set-top box operates in this state until it receives an entitlement message. If the set-top box, being in the undetermined mode, receives the message 284 assigning the mode of acting as a master, the set-top box changes its mode to the 175 master set-top box in a coupled state. When a message 285 assigning the mode of a master set-top box is received, the set-top box changes its mode 176 to that of a master set-top box in a coupled state, retaining this state as long as it is getting messages 286 about coupling. This status is changed when a reset coupling message 281 is obtained and then the set-top box changes its state 172 to undetermined mode and status.

If the set-top box 174 of undetermined mode does not receive 283 a message assigning the master mode, the set-top box changes its mode to act as the slave set-top box 177 having the coupling status. When the coupling message 289 is delivered, the set-top box changes its mode to the slave set-top box 179 with coupled status, retaining this status as long as it is receiving coupling messages 291. This state is modified if either a period of operating video expires and the set-top box is attributed the state of the timeout, or a

reset coupling message 281 is delivered, resulting in a change of the set-top box 172 state to undetermined mode and status.

If the set-top box 177 in the slave mode during the coupling period 288 is not provided with the message 289 about successful coupling, it changes its mode to a slave set-top box 178 with expired operating time. The set-top box remains in this state until it receives a message 290 about coupling.

The access system to the broadcast network presented in fig. 12 comprises the master set-top box 11 and n slave set-top boxes 12, 15 linked to the master set-top box 11. The master set-top box 11 and the set-top boxes 12, 15 have four functional blocks, crucial for the system under discussion. Receiving and processing systems 251, 261, 271 are responsible for receiving a signal from the broadcast network 8. This signal is converted to numerical values and is then sent for further processing. Processors 250, 260, 270 are responsible for the control of all the other systems 253, 263, 273 operating within one set-top box. For example, in fig.12, in the other systems 253, 263, 273, the systems 255, 265, 275 of access control were separated, and the other systems 254, 264, 274, which can be audio and video decoders, including those of MPEG and AC/3 format, systems generating graphics, systems generating audio and video output signals for a TV receiver, systems of memory (RAM, ROM, Flash, HDD), systems controlling outer interfaces (keyboard, remote control unit), systems controlling a return channel. Processors 250, 260, 270 execute software controlling the work of these systems and also control demultiplexers 252, 262, 272 operating within the private network 13 used to send different information. The private network 13 can share physical media with the broadcast network 8 and in this case the demultiplexers 252, 262, 272 become an integral part of the receiving and processing system operating within the broadcast network 8.

Fig. 12 illustrates an example of a way of message transmission between two systems of access control 255 and 265 of two different set-top boxes 11 and 12. In the situation illustrated in fig. 12, the access control system 255 of the master set-top box 11 transmits a message to the access control system 265 of the first slave set-top box 12. This message, generated by the

application of the access control system 255, and then transmitted by the application of the demultiplexer 252, is transported over the private network 13. The transmitted message is received by the demultiplexers 262, 272 of the remaining set-top boxes 12, 15. The first slave set-top box 12, which received the message through the route 281, accepts this message, while the n-th slave set-top box 15, which received this message through the route 282, rejects it. Next, the application of the access control system 265 of the first slave set-top box 12 begins to process the message received from the access control system 255 of the master set-top box 11.

Fig. 13 presents an example of a way of message transmission between a device B 277 of the n-th slave set-top box 15 and an external device A 267 linked to the first slave set-top box 12 using an interface A 266 (for example a parallel port, an outer IP network, a wireless connection i.e. Bluetooth or infrared link, or a specific connection assigned to a given type of a device i.e. a Smart-Card connection). The device A 267 linked to the first set-top box 12 sends a message to the device B 277 which receives the message through the route 286. Simultaneously, this message is sent using the route 285 to the master set-top box 11 and is rejected because it is not dedicated to that set-top box.

An exemplary format of a message sent between two set-top boxes is presented in fig. 14. Only the field types of which the message is composed have been shown, without specifying their sizes. The precise format of a particular field can be adapted to suit a specific solution.

An exemplary message, beginning from the top, consists of synchronising bytes 300 which are used for identification of a new message. Therefore they should be unique bytes so that they will not appear in a later part of the message. For example, if the message is encoded in the Manchester system, the two bytes of values 0h8E and 0h71 respectively can serve as the synchronising bytes. This combination will not appear in the message encrypted using Manchester system and can be used as a unique characterisation of the beginning of the message.

The next part of the message is a heading 301 which consists of a field describing a destination address 302 of the message, a field describing a source address 303 of the message, a flag 304 with information whether the message contains data or not, a field 305 describing the type of the message, and a field 306 describing the length of a payload 307.

The last field is a checksum 308 which is used to detect and/or correct an error that can appear during the message transmission.

The described message can be addressed to a particular set-top box or to all set-top boxes. Information within the message can be placed in the block of data or in the block describing the type of message (messages without payload are the control and confirmation messages)

The preparation process of the message described above is presented in fig.15 in the form of a block diagram.

The message formation starts in step 311 where the message is generated by a program, which is going to send the message. In step 312 the program creates the message, i.e. forms the heading with source and destination addresses, type and length of attached data. Next it adds data, and finally calculates the code of the checksum for the whole message. The procedure of message transmission starts in step 313.

The messages, which were sent, are delivered to the demultiplexer, which analyses the state of the private network 13 waiting to receive transmitted messages.

The procedure of message reception and analysis presented in fig. 16 starts in step 401 where the demultiplexer receives an incoming message. In step 402 the demultiplexer checks if the form of the delivered message is correct. The transmission error can be a result of a collision between two simultaneously sent messages. For this reason the format of message is verified and it is checked if data, at least in the heading, are not corrupt. The verification process is based on the analysis of the checksum. If in step 403 it emerges that the message is damaged, the message is rejected in step 404. If the message is in a correct form, in step 405 the heading is analysed, by reading the data concerning the destination address. It is decided in step 406

whether the message is dedicated to this particular set-top box. In case the message is not dedicated to this set-top box, the rejection follows in step 407. If the message is dedicated to the given set-top box it is read in step 408. Next, it is verified in step 409 if the given type of the message can be used by the set-top box. If the message has been sent to all set-top boxes, but one of them does not have a device to support the processing of this message, in step 410 the message is rejected. However, if the given type of message can be processed by the set-top box, in step 411 the message is passed to the software responsible for certain functions or operation of a particular device.

The described solution relies on the set-top box management system which generates the message coupling the master set-top box with the slave set-top box or boxes, and the security system for encrypting and decrypting data sent from the master to the slave through the private network. The management system of set-top boxes generates messages for each pair of the master and the slave set-top box as well as the code for the transmission.

The most practical and characteristic features of the solution are the identification method of master and slave set-top boxes and the coupling between each pair of set-top boxes, which are realised with the use of the number of the smart card assigned individually to each set-top box. The newly installed set-top box is operationally neutral either within specific period of time or until the message assigning its role is delivered. If no message is received within the predetermined period of time, the set-top box is disabled. Because the master set-top box has to contact the slave set-top box to activate it, the disabled slave set-top box can operate again as soon as it becomes connected to the master set-top box, which is able to identify the proximity of the slave within the broadcasting network and which is also able to use this intelligence to disable the slave set-top box that has been moved. The coupling can be reset anytime through the broadcasting network.

CLAIMS

1. A broadcast network access-management system comprising at least one master decoding device provided with a smart card, and at least one slave decoding device linked to it, and a transmitter device which generates and transmits entitlement management messages intended for the linked master and slave decoding devices and other devices characterised in that the master decoding device (11) and at least one slave decoding device (12) linked together are located in a defined distance and operate when a distance between them does not exceed the defined distance dependant upon a cable length, a configuration, a number and a quality of splitters and connections.
2. The broadcast network access-management system, according to claim 1, in which a decoding device is assigned the status of the master decoding device (11) only after it has been linked to a network and an entitlement control message for the master decoding device (11) has been found.
3. The broadcast network access-management system, according to claim 1, in which the master decoding device (11) imposes on the transmitter device (3) a transmission of the entitlement control message appropriate for the master decoding device (11).
4. The broadcast network access-management system, according to claim 1, in which a decoding device is granted with a mode of the slave decoding device (12) only after it has been linked to a network and an entitlement control message for the slave decoding device (12) has been found.
5. The broadcast network access-management system, according to claim 1, in which the slave decoding device (12) imposes on the transmitter device (3) a transmission of the entitlement control message appropriate for the slave decoding device (12).

6. The broadcast network access-management system, according to claim 1, in which the master decoding device (11) and the slave decoding device (12), when they are turned on, first check if any messages are being transmitted by other devices before they start to transmit messages.
7. The broadcast network access-management system, according to claim 1, in which the slave decoding device (12) triggers the master decoding device (11) to transmit the entitlement control message appropriate for the slave decoding device (12) and messages with demand for coupling.
8. The broadcast network access-management system, according to claim 1, in which a period of time for coupling the master decoding device (11) with the slave decoding device (12) is pre-set.
9. The broadcast network access-management system, according to claim 1, in which the defined distance between the master decoding device (11) and the slave decoding device (12) linked to it is determined from the level of a signal exchanged between the master decoding device (11) and the slave decoding device (12).
10. The broadcast network access-management system, according to claim 1, in which the level of the signal exchanged between the master decoding device (11) and the slave decoding device (12) is compared with the level of the signal sent between them during preceding communication.
11. The broadcast network access-management system, according to claim 1, in which decoding devices are assigned the status of the master decoding device (11) and the slave decoding device (12) after transmission of encoded messages by the transmitter device (3) generating and transmitting specified codes.

12. The broadcast network access-management system, according to claim 1, in which a private television network (13) shares physical linkages with a broadcast network (3).

13. The broadcast network access-management system, according to claim 1, in which the entitlement management messages, allowing the master decoding device (11) and at least one slave decoding device (12) an access to the broadcast network, are transmitted after the encoded messages are sent by the transmitter device (3) which is designed to generate and transmit specific codes.

14. The broadcast network access-management system, according to claim 1, in which management messages sent to the master decoding device (11) and the slave decoding device (12) are generated by a generator (7) connected to a multiplexer (5) through another generator (6) which creates messages, and the management messages sent to the master decoding device (11) and the slave decoding device (12) are included in the entitlement management message.

15. The broadcast network access-management system, according to claim 1, in which messages exchanged between the master decoding device (11) and the slave decoding devices (12, 15) are messages used to identify the master decoding device (11) and the slave decoding devices (12, 15), systems that are their component parts, or external devices (267) linked to them.

16. The broadcast network access-management system, according to claim 1, in which the identifying messages include a type of the master decoding device (11) and the slave decoding devices (12, 15), their version and/or their serial number.

17. The broadcast network access-management system, according to claim 1, in which messages exchanged between the master decoding device (11)

and the slave decoding devices (12, 15) are messages used to identify software.

18. The broadcast network access-management system, according to claim 1, in which the messages used to identify software include a version number and/or a serial number of the software.

19. The broadcast network access-management system, according to claim 1, in which messages exchanged between the master decoding device (11) and the slave decoding devices (12, 15) are messages facilitating interaction between the decoding devices (11, 12, 15), systems integral to them, or between software installed in the decoding devices (11, 12, 15) or devices co-operating with them.

20. The broadcast network access-management system, according to claim 1, in which messages exchanged between the master decoding device (11) and the slave decoding devices (12, 15) are messages which incorporate an operating status of a given device/program, a result of a certain operation, an order to execute a certain operation and data collected or processed by a certain device/software.

21. The broadcast network access-management system, according to claim 1, in which messages exchanged between the master decoding device (11) and the slave decoding devices (12, 15) are messages generated either within the decoding devices (11, 12, 15) or delivered from external sources.

22. The broadcast network access-management system, according to claim 1, in which messages exchanged between the master decoding device (11) and the slave decoding devices (12, 15) are internet data, text messages, streams and files containing sound, pictures, video and software, and/or updates of software.

23. The broadcast network access-management system, according to claim 1, in which messages exchanged between the master decoding device (11) and the slave decoding devices (12, 15) contain additional messages generated by software installed in the decoding device or devices which are co-operating with them, or the messages which are delivered to the decoding devices from outside sources.

24. The broadcast network access-management system, according to claim 1, in which messages exchanged between the master decoding device (11), the slave decoding devices (12), and outside devices consist of synchronising bytes (300), a heading (301) with a source and a destination addresses (302, 303), a type (305) of message, a flag (304) with information as to whether the message contains data and the message (306) determining the size of the block of data, and also data (307) constituting the message (referred to as a payload), and a checksum (308).

25. A management method of receivers provided with smart cards and linked to a television broadcast network, among which at least one device is the master decoding device with at least one slave decoding device and an interlinked transmitter device which generates and transmits messages that allow to use the master and the slave decoding devices and receivers connected to them, the management method comprising the following steps:
installing the master decoding device (11) and at least one linked slave decoding device (12) at a defined distance from each other shorter than a defined nominal distance;
allowing the master decoding device (11) and the slave decoding device (12) to operate only if a distance between the master decoding device (11) and the slave decoding device (12) distance does not exceed the defined nominal distance dependant upon a cable length, a number, a configuration and a quality of splitters and links.

26. The management method, according to claim 25, characterized in that a decoding device is assigned the status of the master decoding device (11) only after it has been linked to a network and an entitlement control message for the master decoding device (11) has been found.

27. The management method, according to claim 25, characterized in that the master decoding device (11) imposes on the transmitter device a transmission of the entitlement control message appropriate for the master decoding device (11).

28. The management method, according to claim 25, characterized in that a decoding device is granted with a mode of the slave decoding device (12) only after it has been linked to a network and an entitlement control message for the slave decoding device (12) has been found.

29. The management method, according to claim 25, characterized in that the slave decoding device (12) imposes on the transmitter device a transmission of the entitlement control message appropriate for the slave decoding device (12).

30. The management method, according to claim 25, characterized in that the master decoding device (11) and the slave decoding device (12), when they are turned on, first check if any messages are being transmitted by other devices before they start to transmit messages.

31. The management method, according to claim 25, characterized in that the slave decoding device (12) triggers the master decoding device (11) to transmit the entitlement control message appropriate for the slave decoding device (12) and messages with demand for coupling.

32. The management method, according to claim 25, characterized in that a period of time for coupling the master decoding device (11) with the slave decoding device (12) is pre-set.

33. The management method, according to claim 25, characterized in that the defined distance between the master decoding device (11) and the slave decoding device (12) linked to it is determined from the level of a signal exchanged between the master decoding device (11) and the slave decoding device (12).

34. The management method, according to claim 25, characterized in that the level of the signal exchanged between the master decoding device (11) and the slave decoding device (12) is compared with the level of the signal sent between them during preceding communication.

35. The management method, according to claim 25, characterized in that decoding devices are assigned the status of the master decoding device (11) and the slave decoding device (12) after transmission of encoded messages by the transmitter device (3) generating and transmitting specified codes.

36. The management method, according to claim 25, characterized in that a private television network (13) shares physical linkages with a broadcast network (8).

37. The management method, according to claim 25, characterized in that the entitlement management messages, allowing the master decoding device (11) and at least one slave decoding device (12) an access to the broadcast network, are transmitted after the encoded messages are sent by the transmitter device (3) which is designed to generate and transmit specific codes.

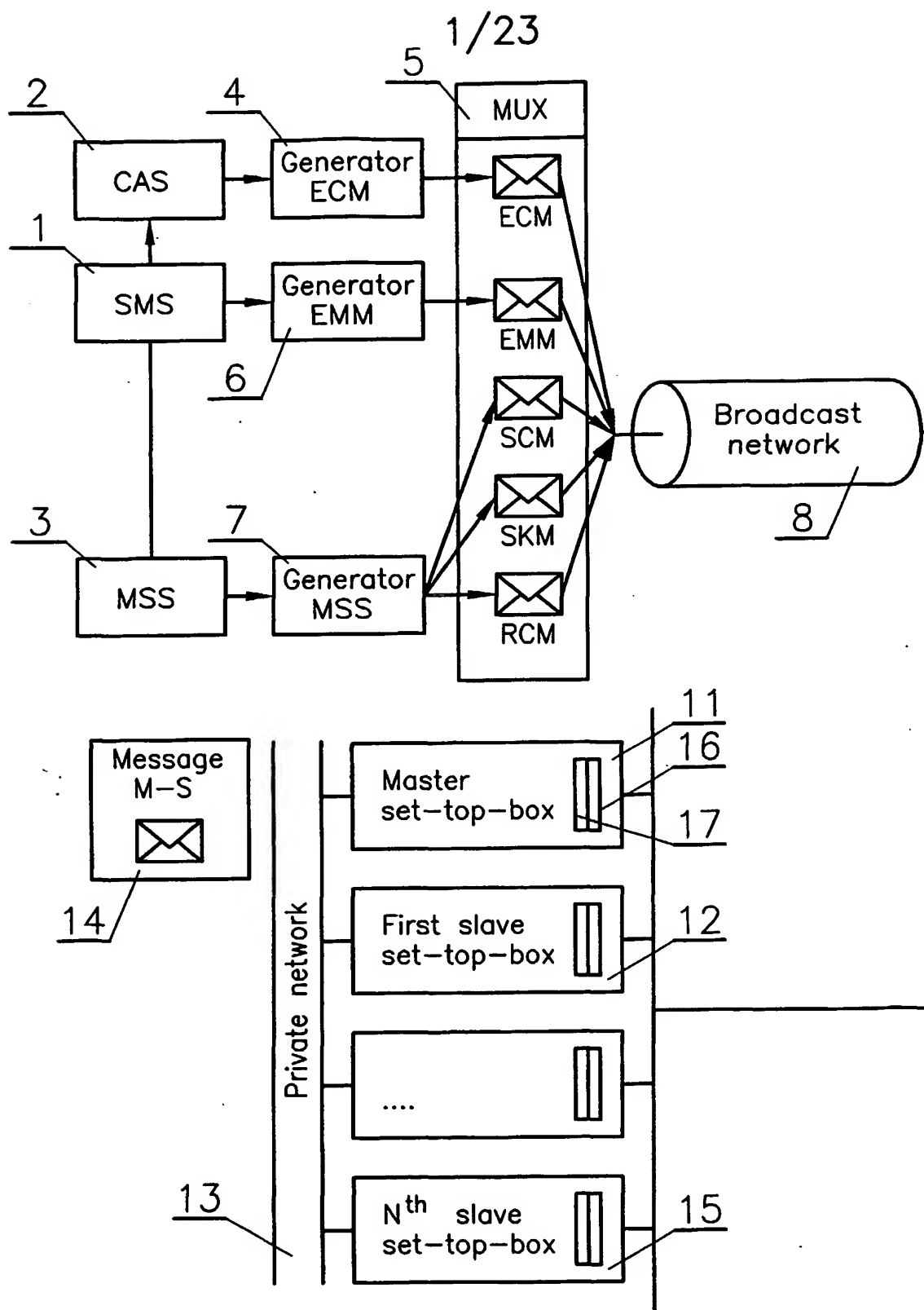
38. The management method, according to claim 25, characterized in that management messages sent to the master decoding device (11) and the slave decoding devices (12) are generated by a generator (7) connected to a multiplexer (5) through another generator (6) which creates messages, and the management messages sent to the master (11) and the slave decoding devices (12) are included in the entitlement management message.

39. The management method, according to claim 25, characterized in that messages exchanged between the master decoding device (11) and the slave decoding devices (12, 15) are messages used to identify the master decoding device (11) and the slave decoding devices (12, 15), systems that are their component parts, or external devices (267) linked to them.

40. The management method, according to claim 25, characterized in that the identifying messages include a type of the master decoding device (11) and the slave decoding devices (12, 15), their version and/or their serial number.

41. The management method, according to claim 25, characterized in that messages exchanged between the master decoding device (11) and the slave decoding devices (12, 15) are messages used to identify software.

42. The management method, according to claim 25, characterized in that the messages used to identify software include a version number and/or a serial number of the software.



2/23

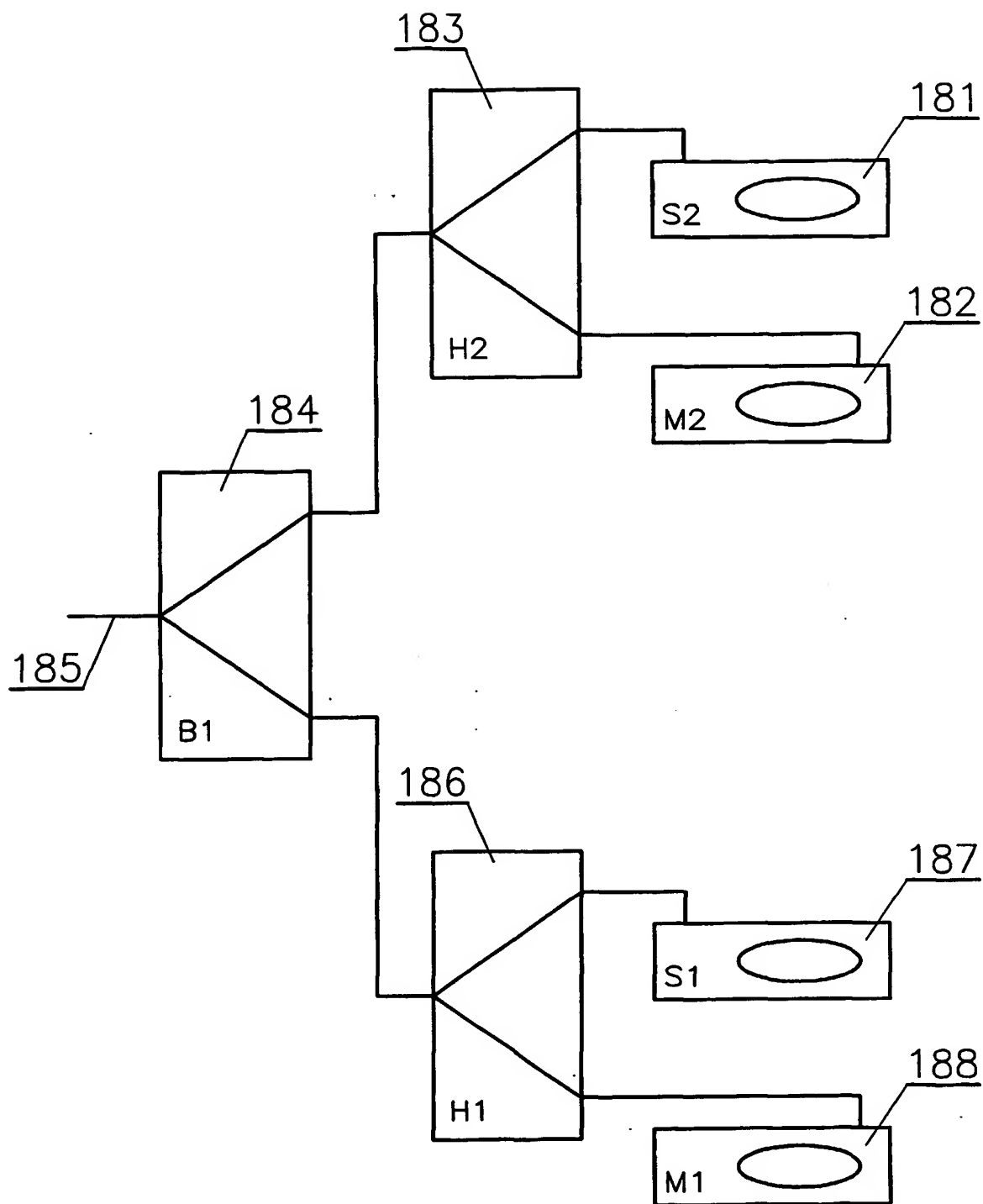


Fig.2

3/23

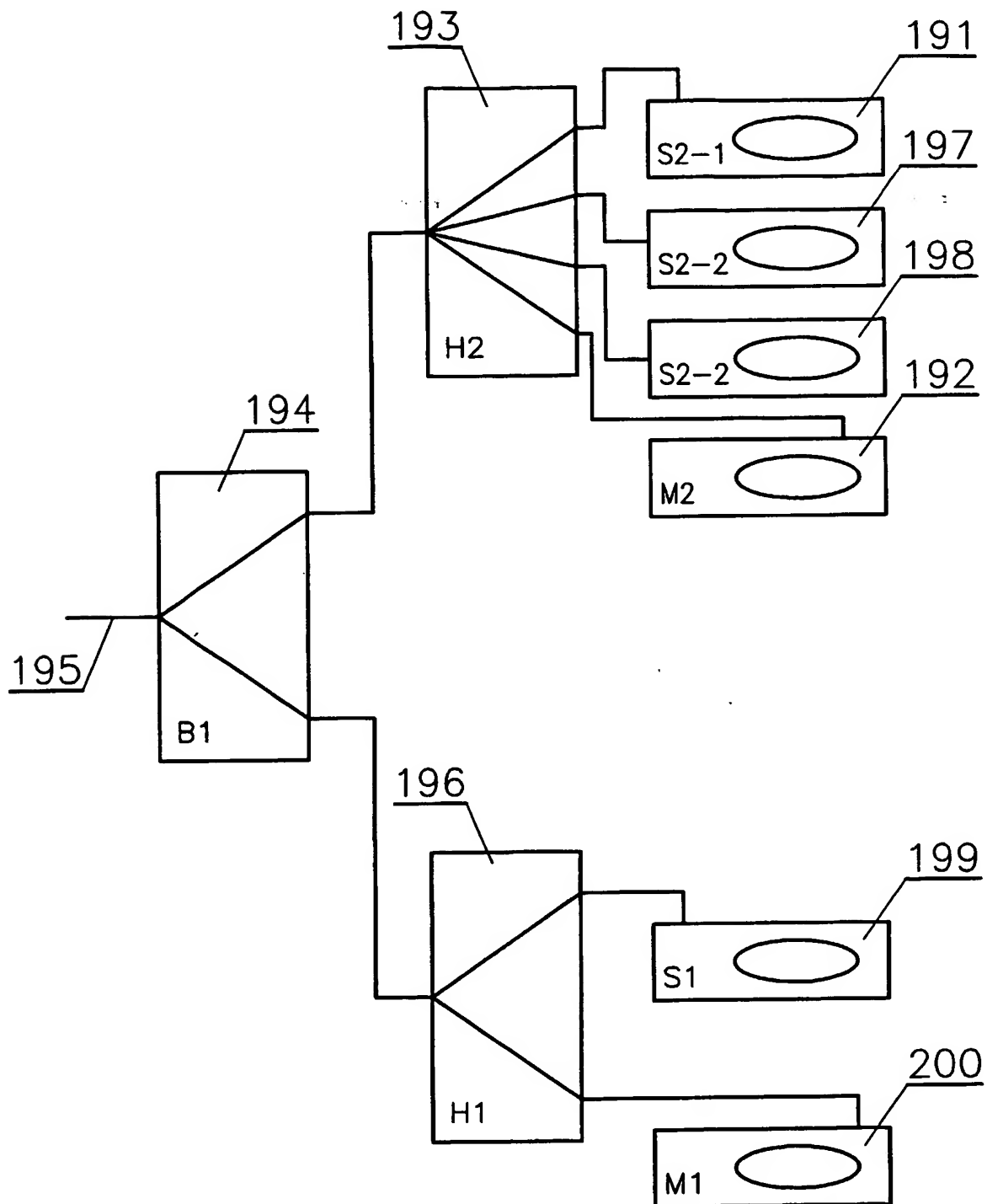


Fig.3

4/23

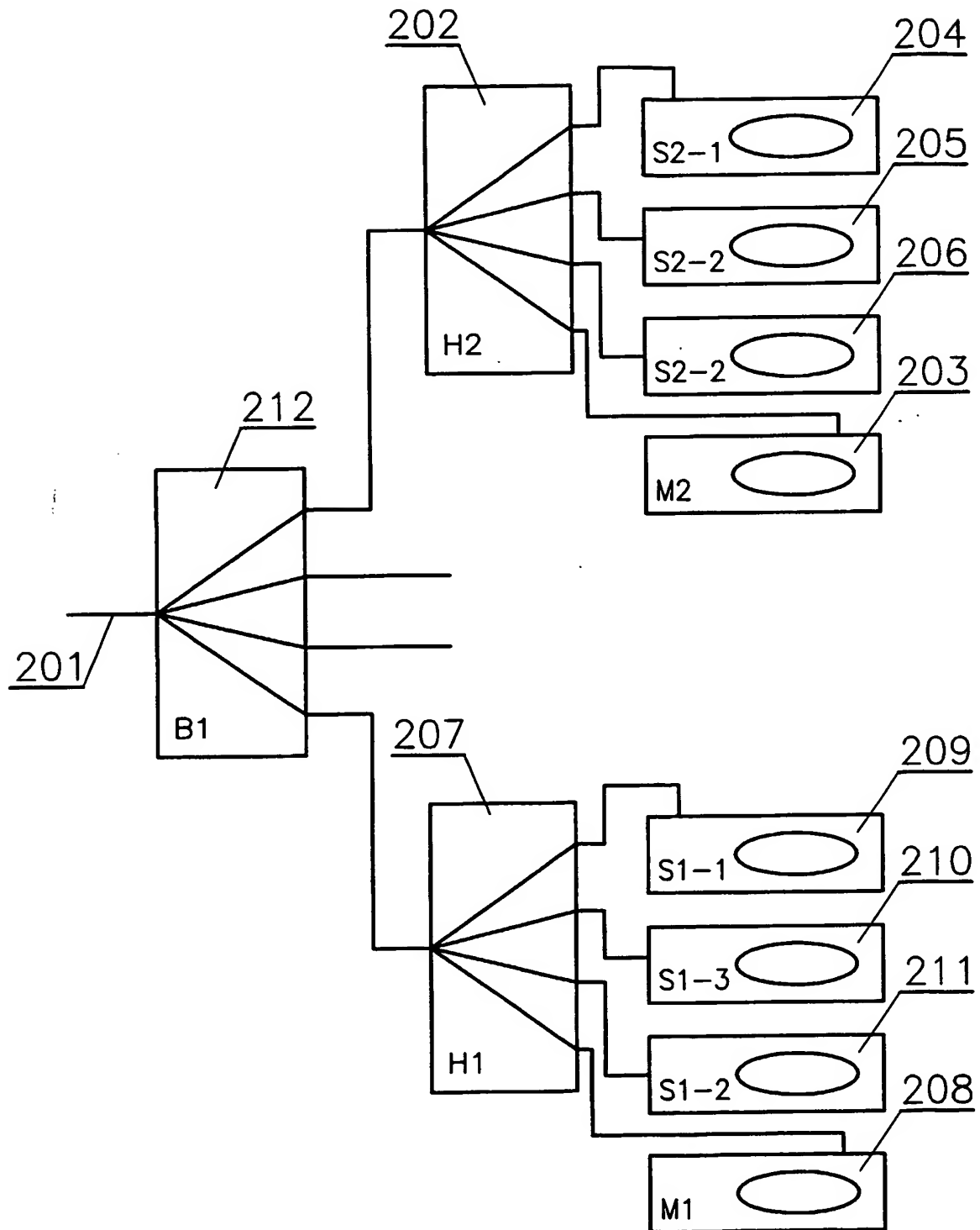


Fig.4

5/23

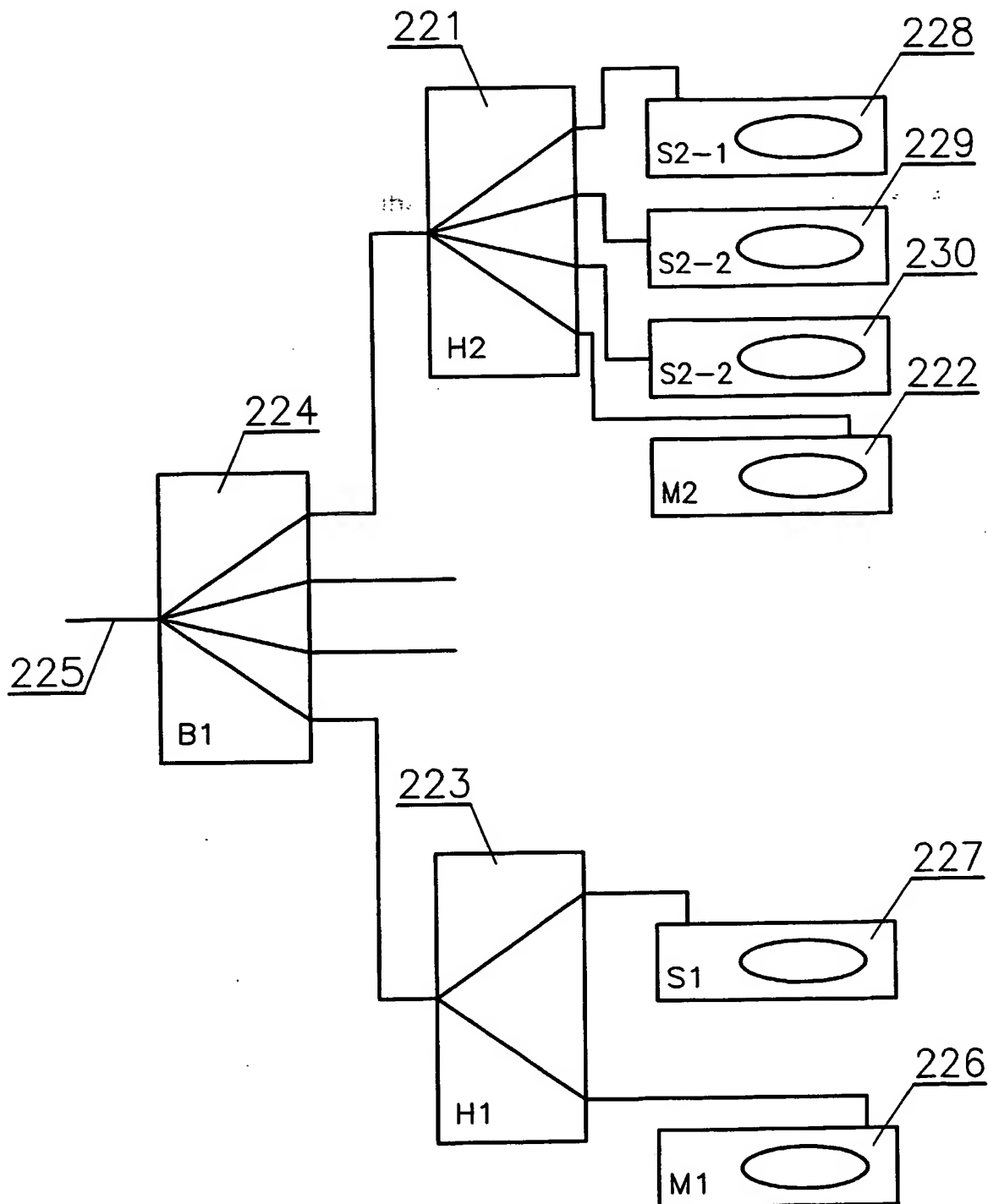


Fig.5

6/23

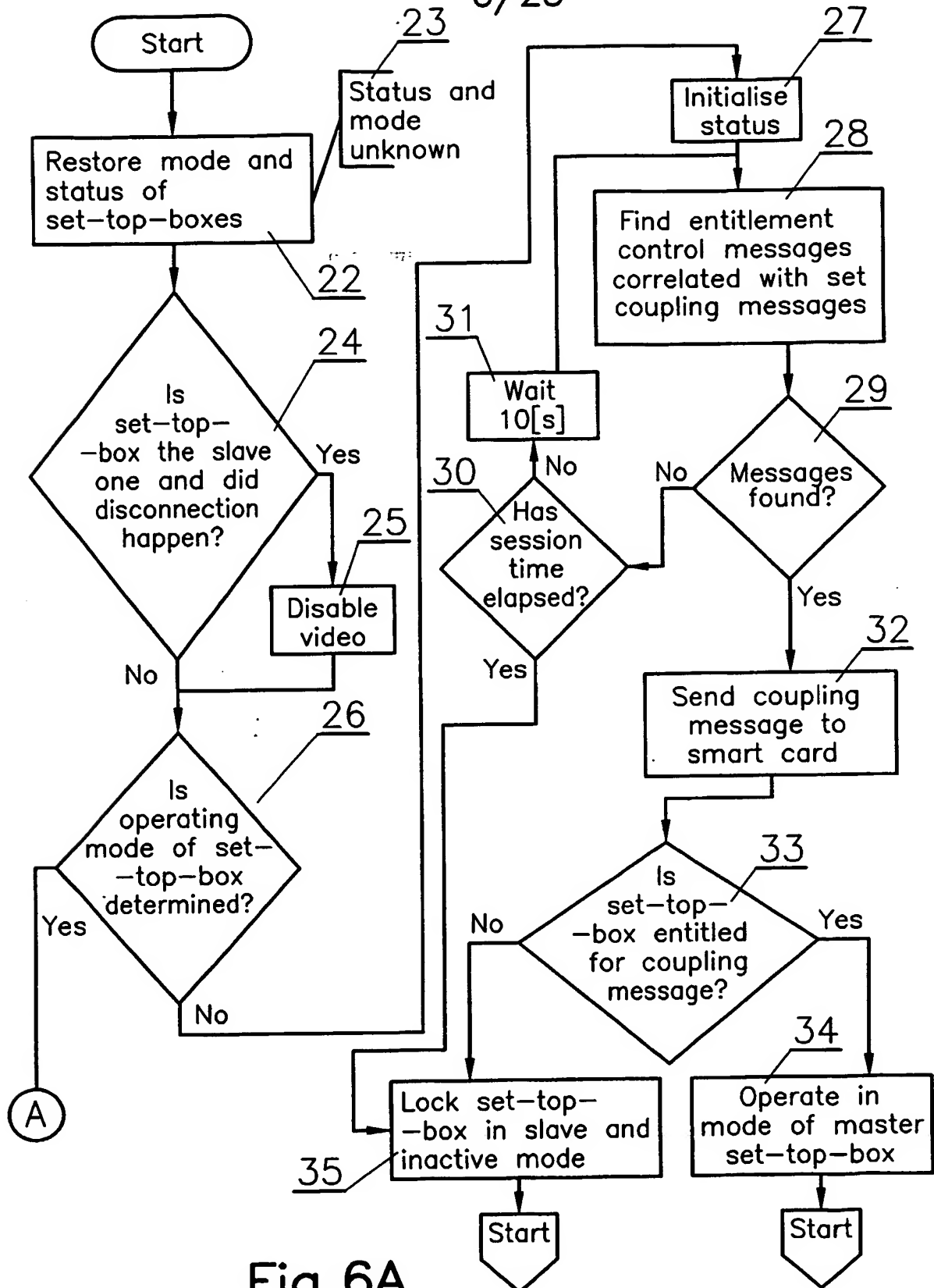


Fig.6A

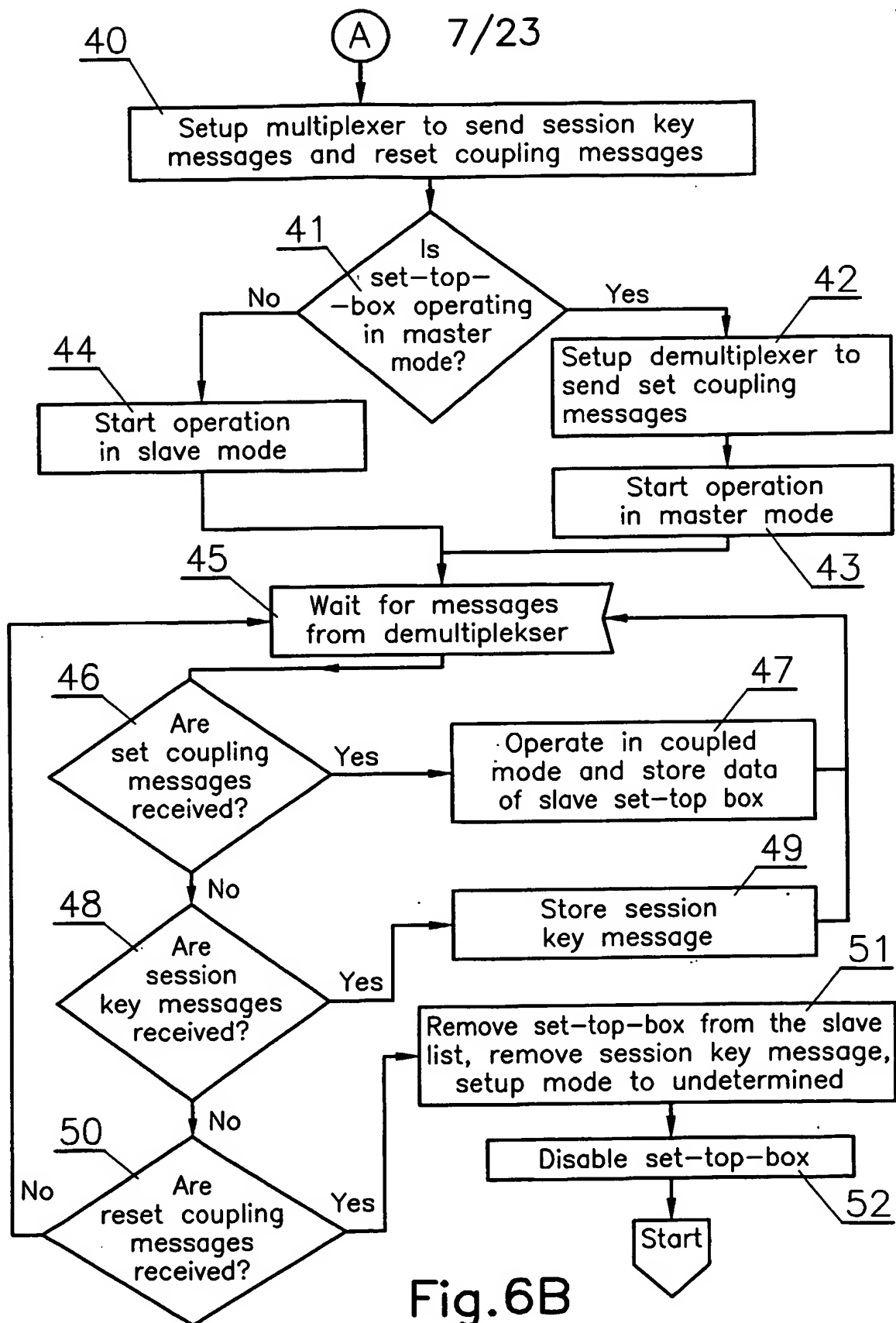


Fig. 6B

8/23

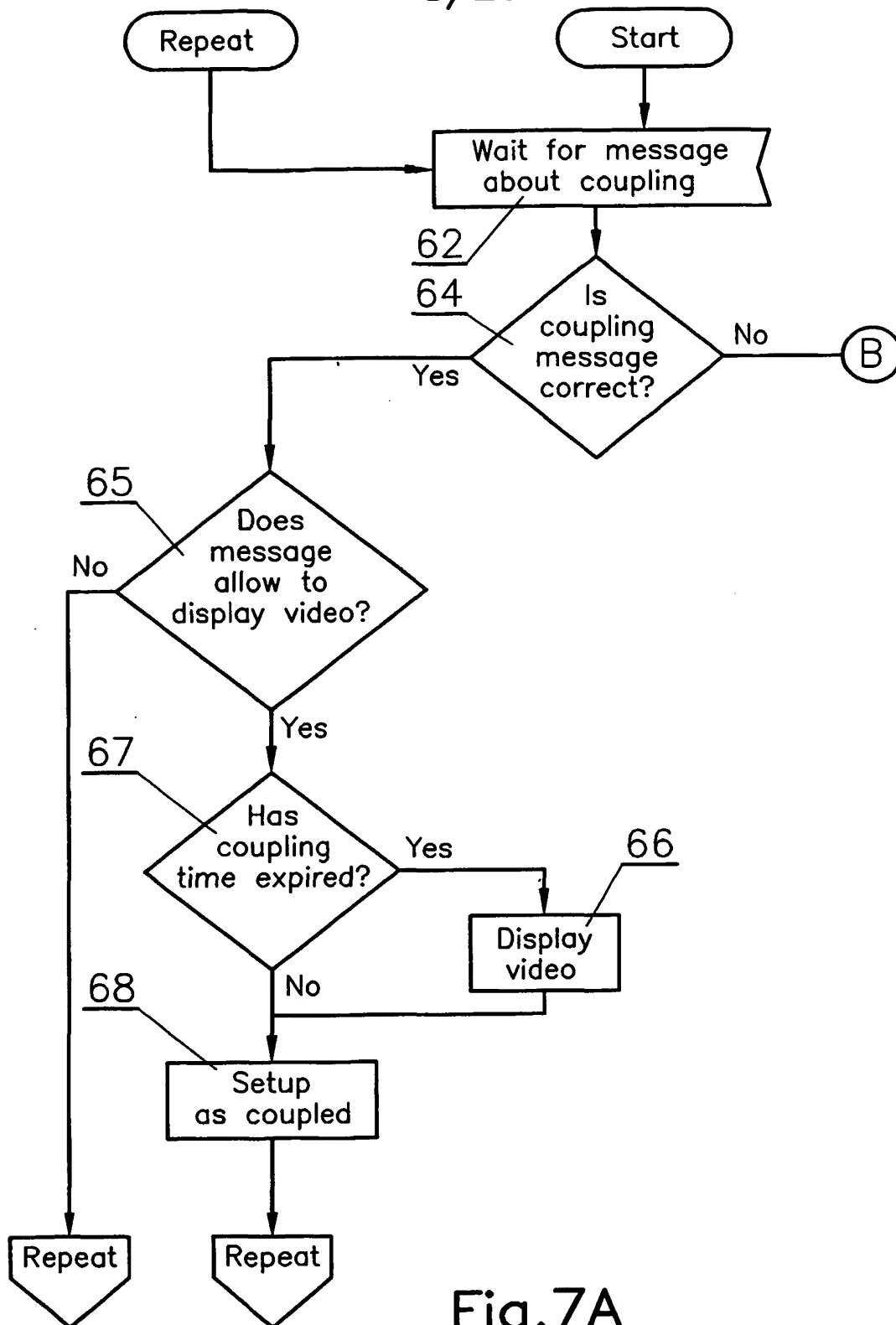
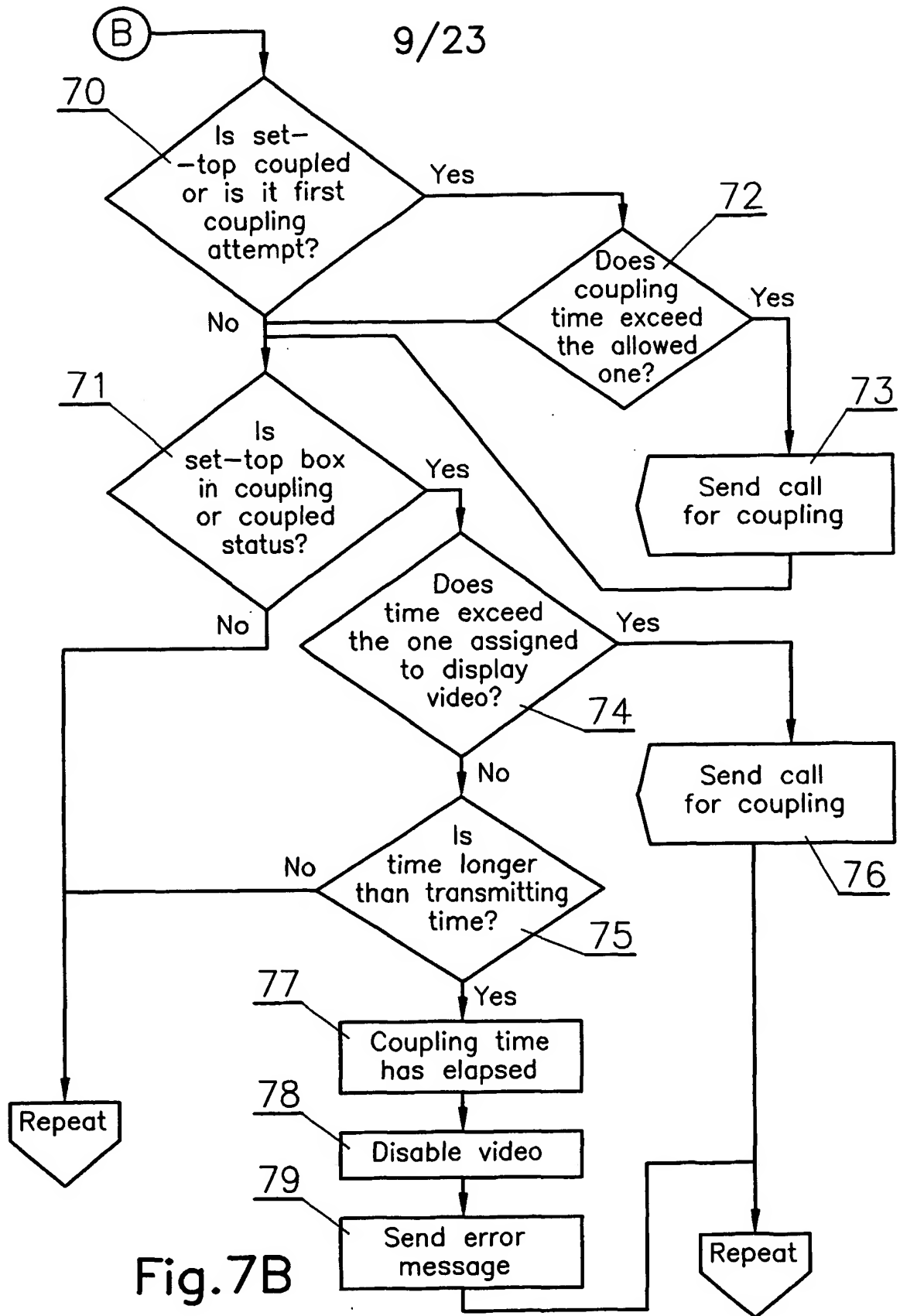


Fig.7A



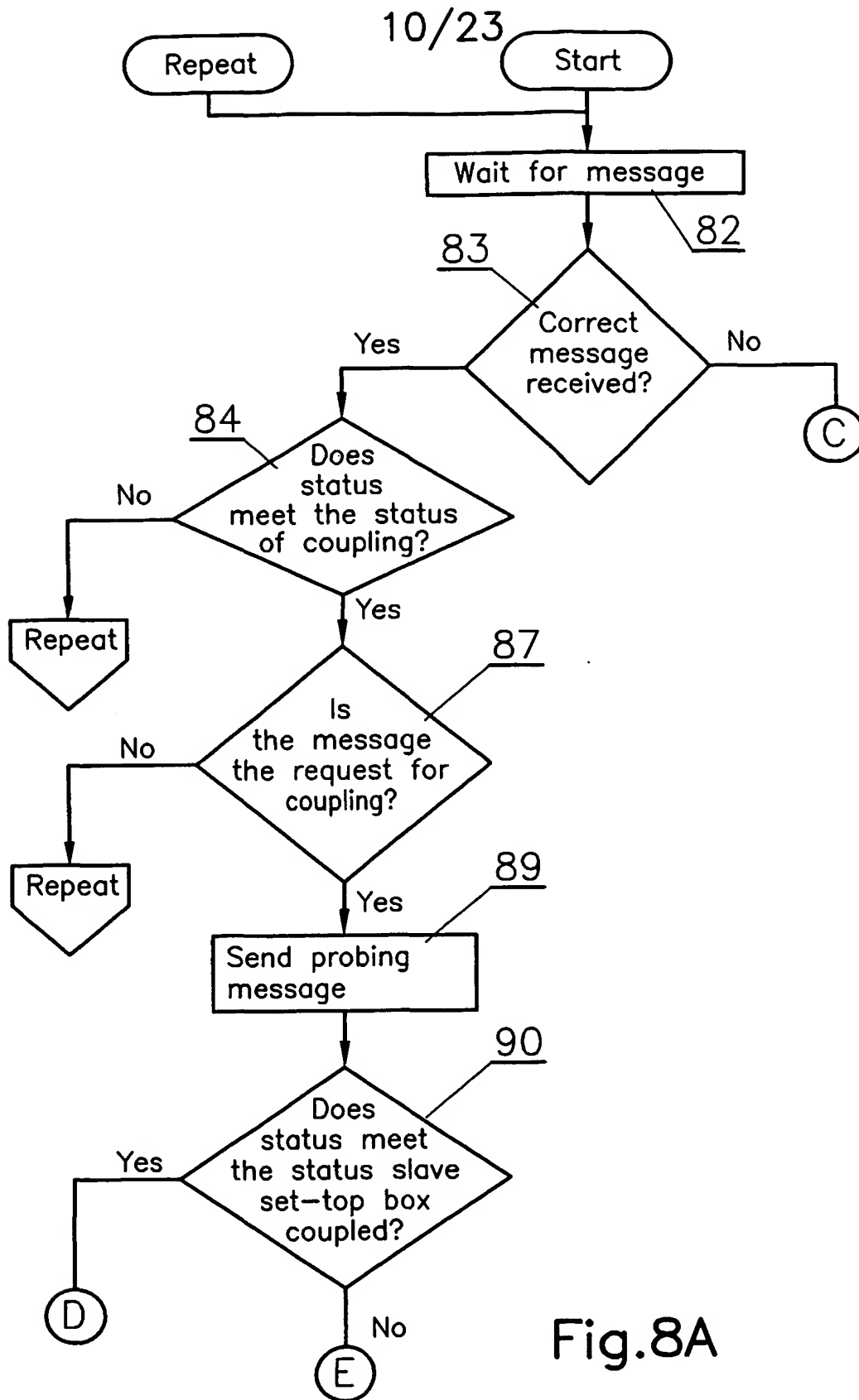


Fig.8A

11/23

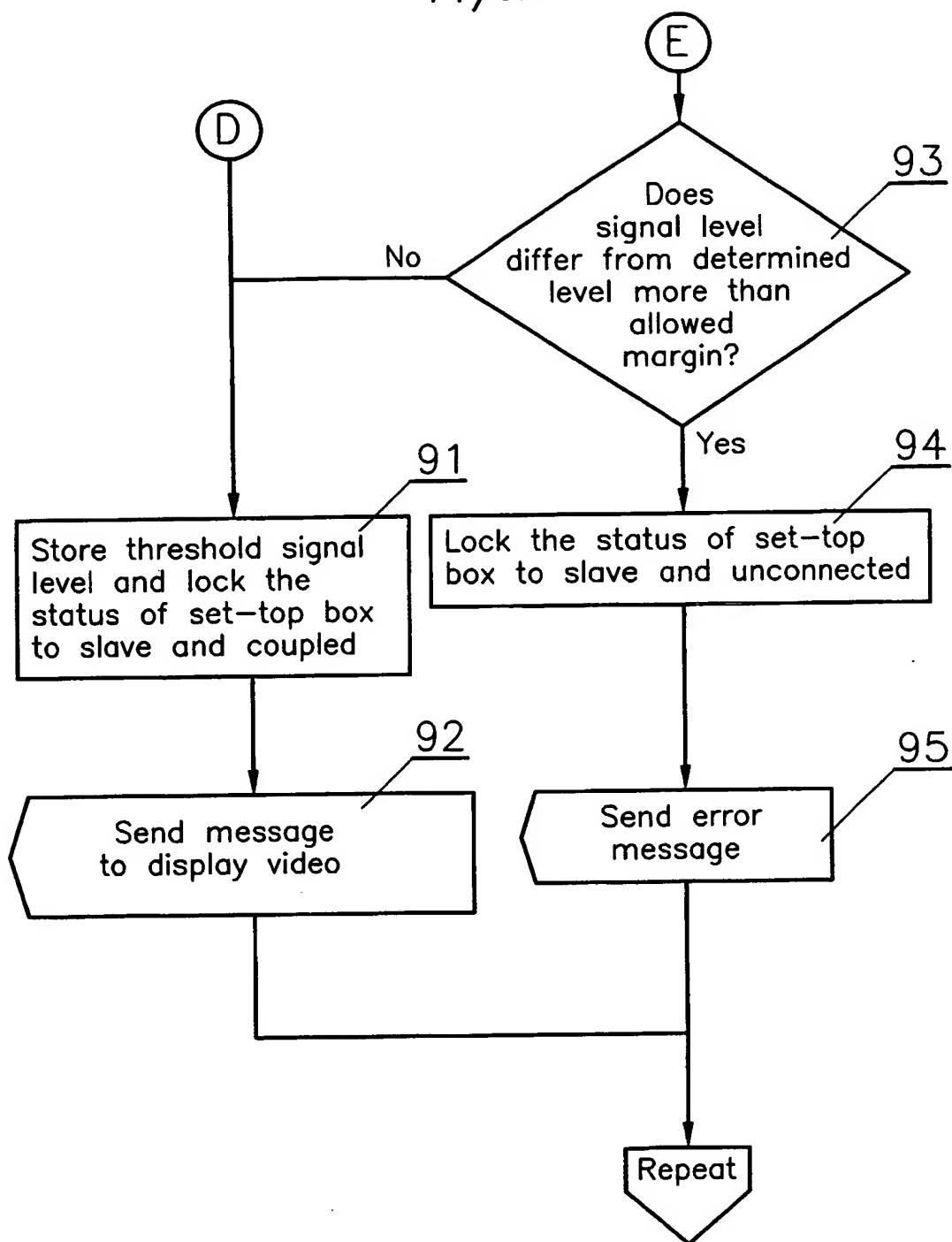


Fig.8B

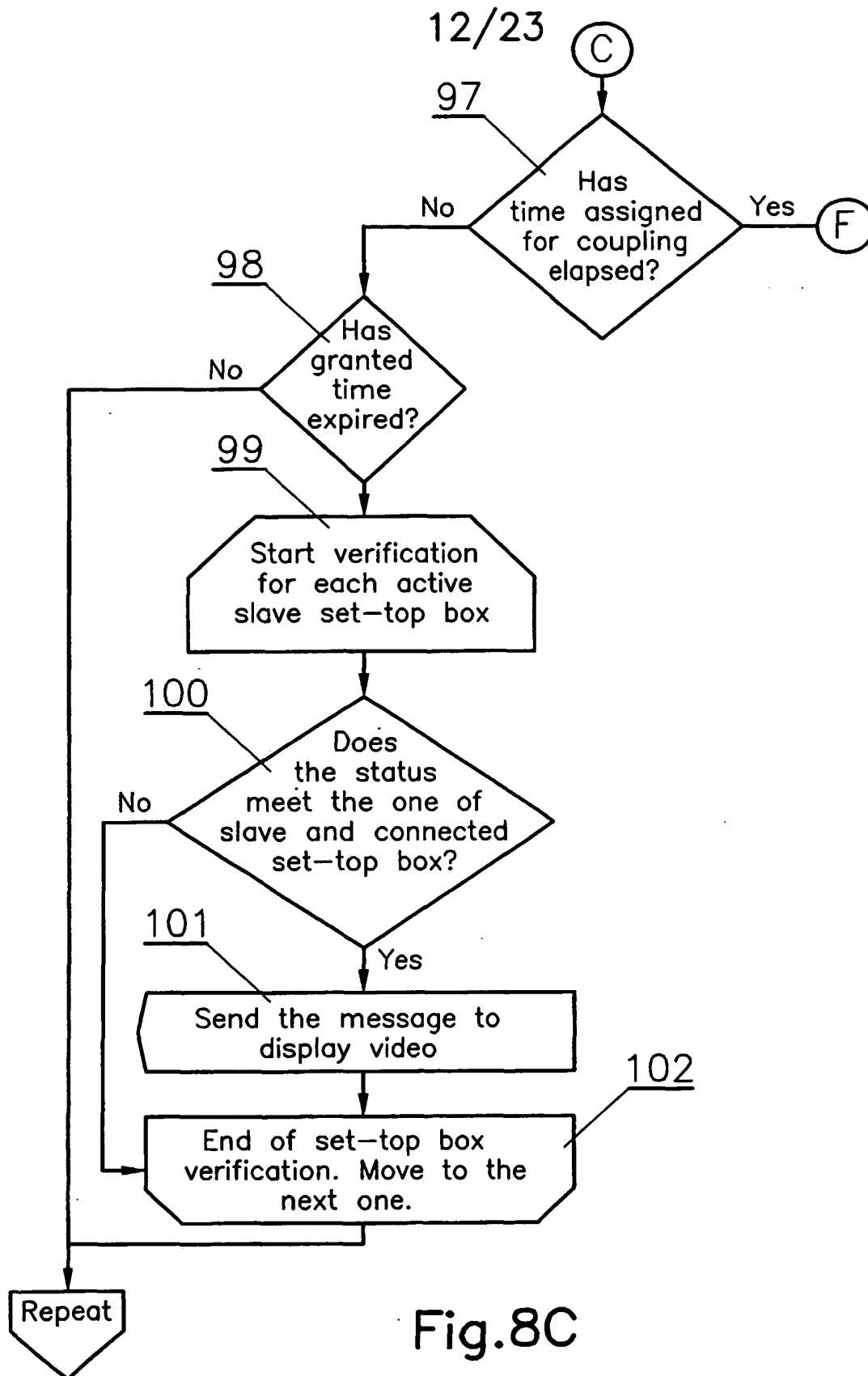


Fig.8C

13/23

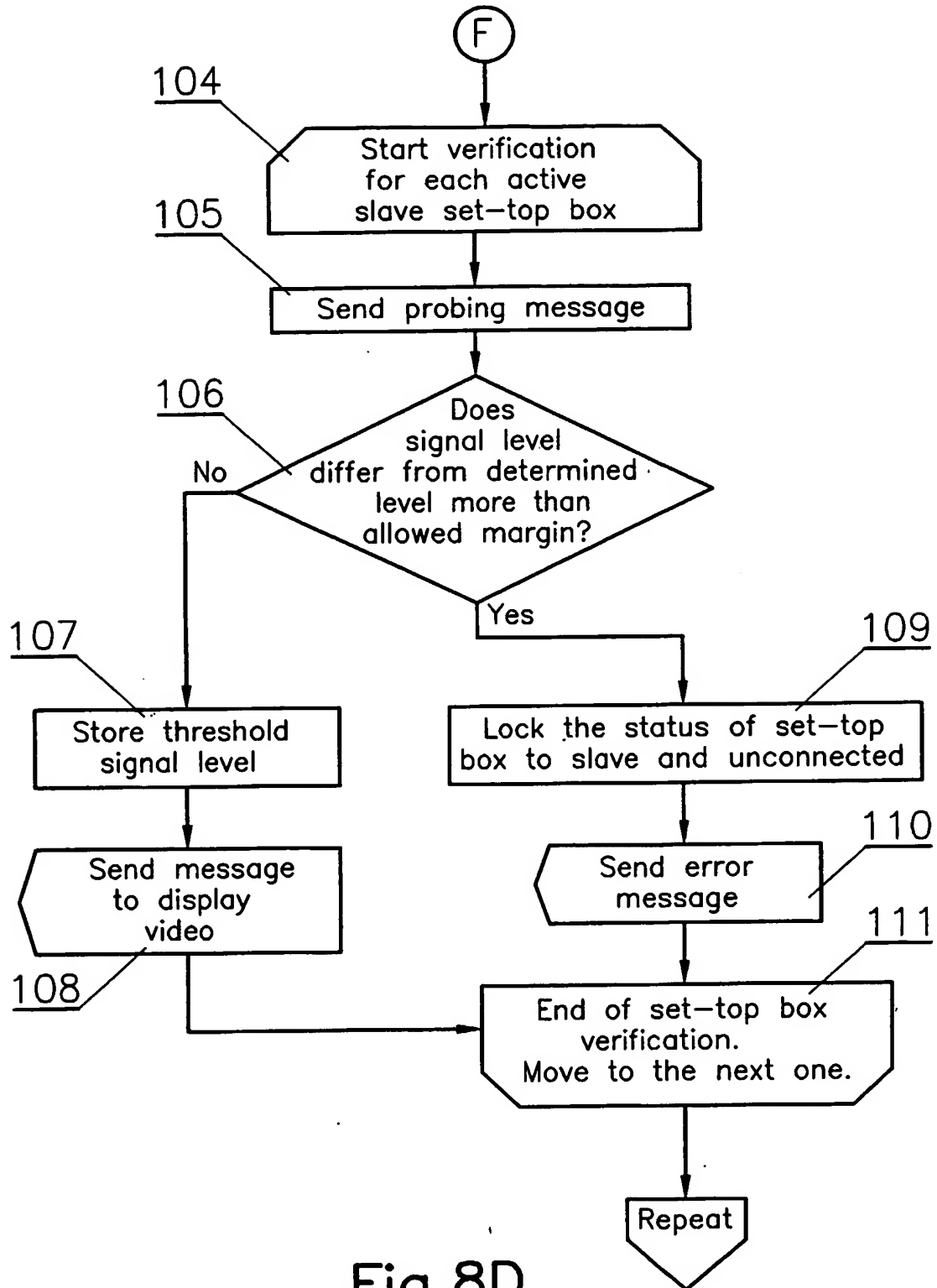


Fig.8D

14/23

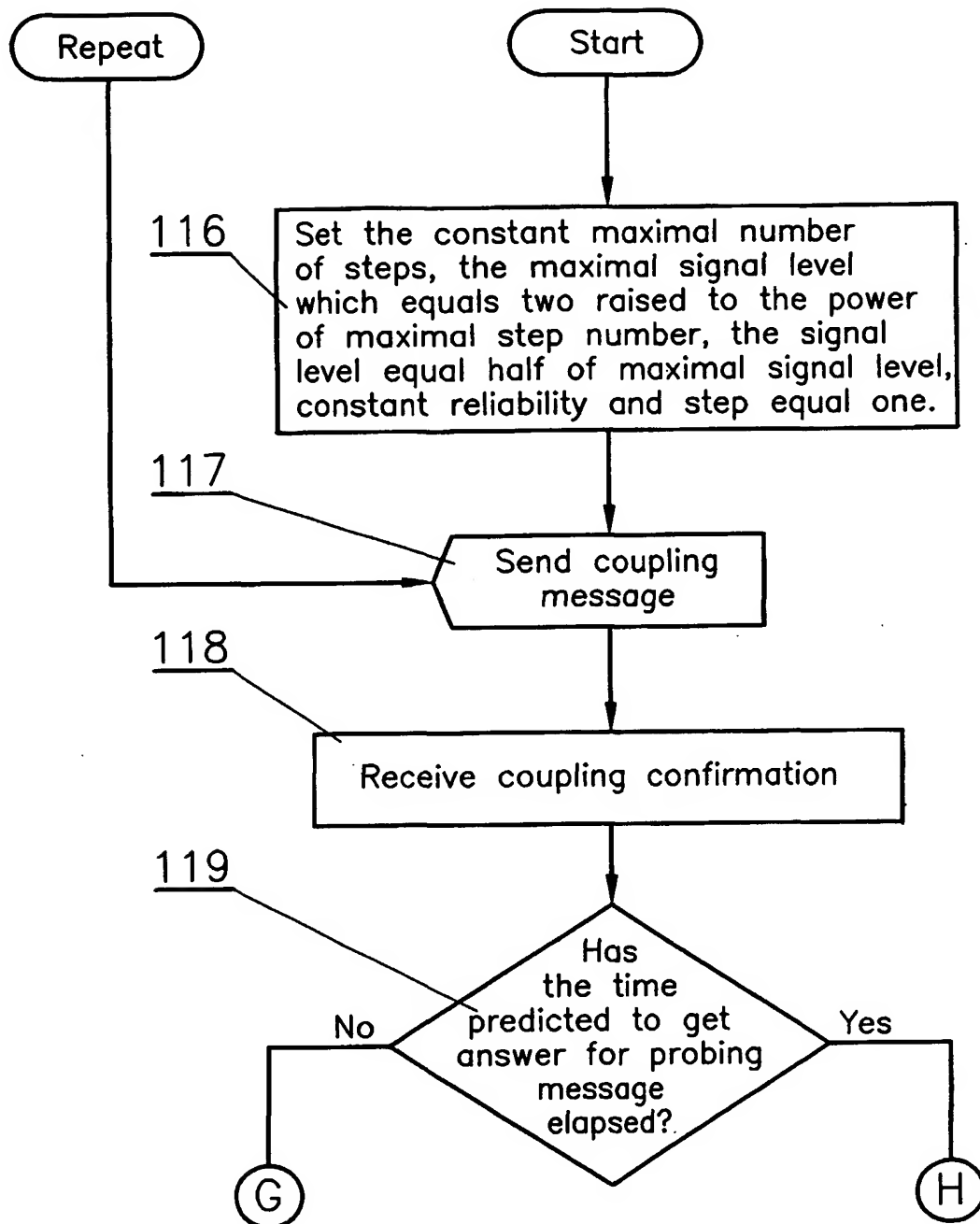


Fig.9A

15/23

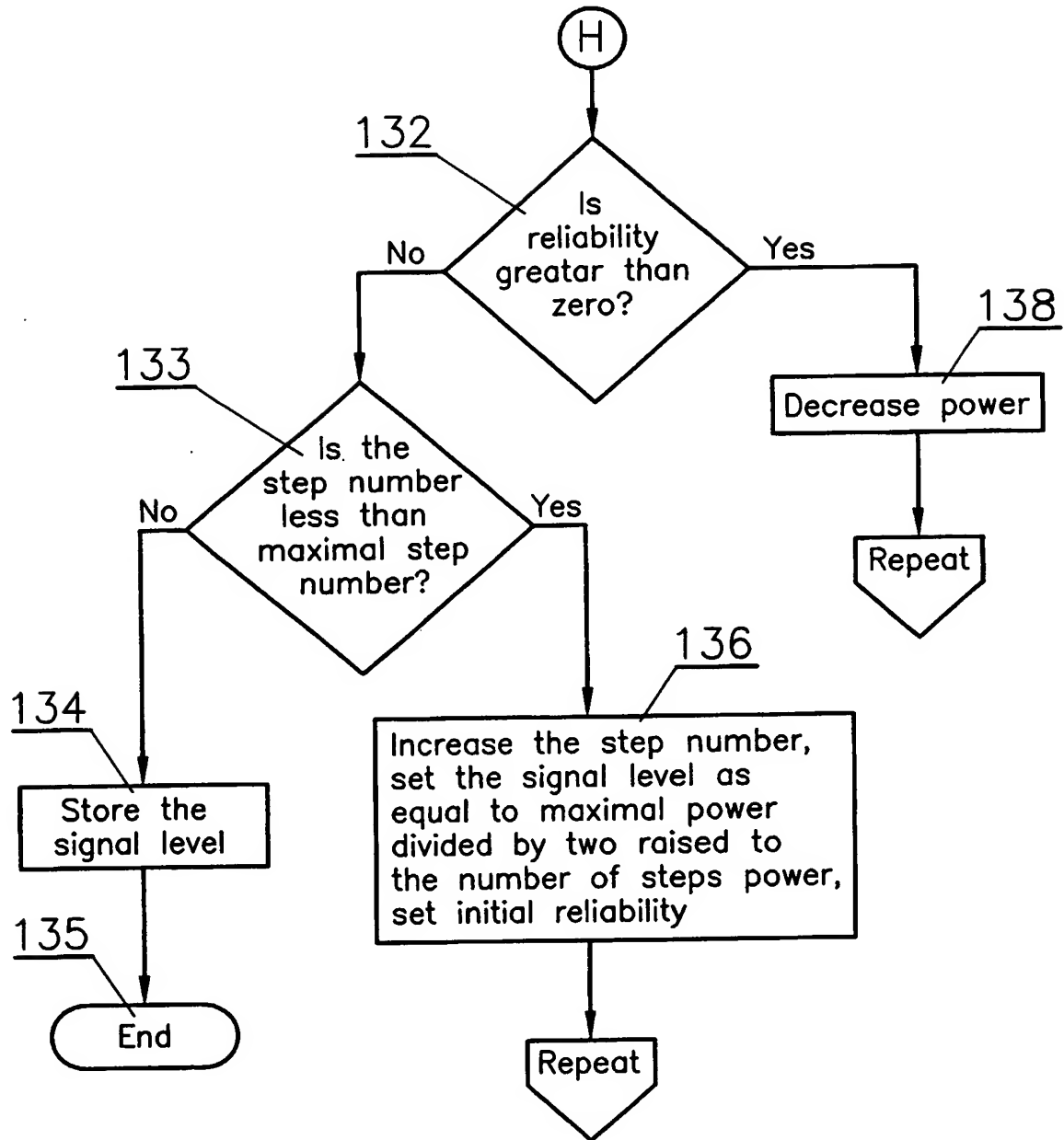


Fig.9B

16/23

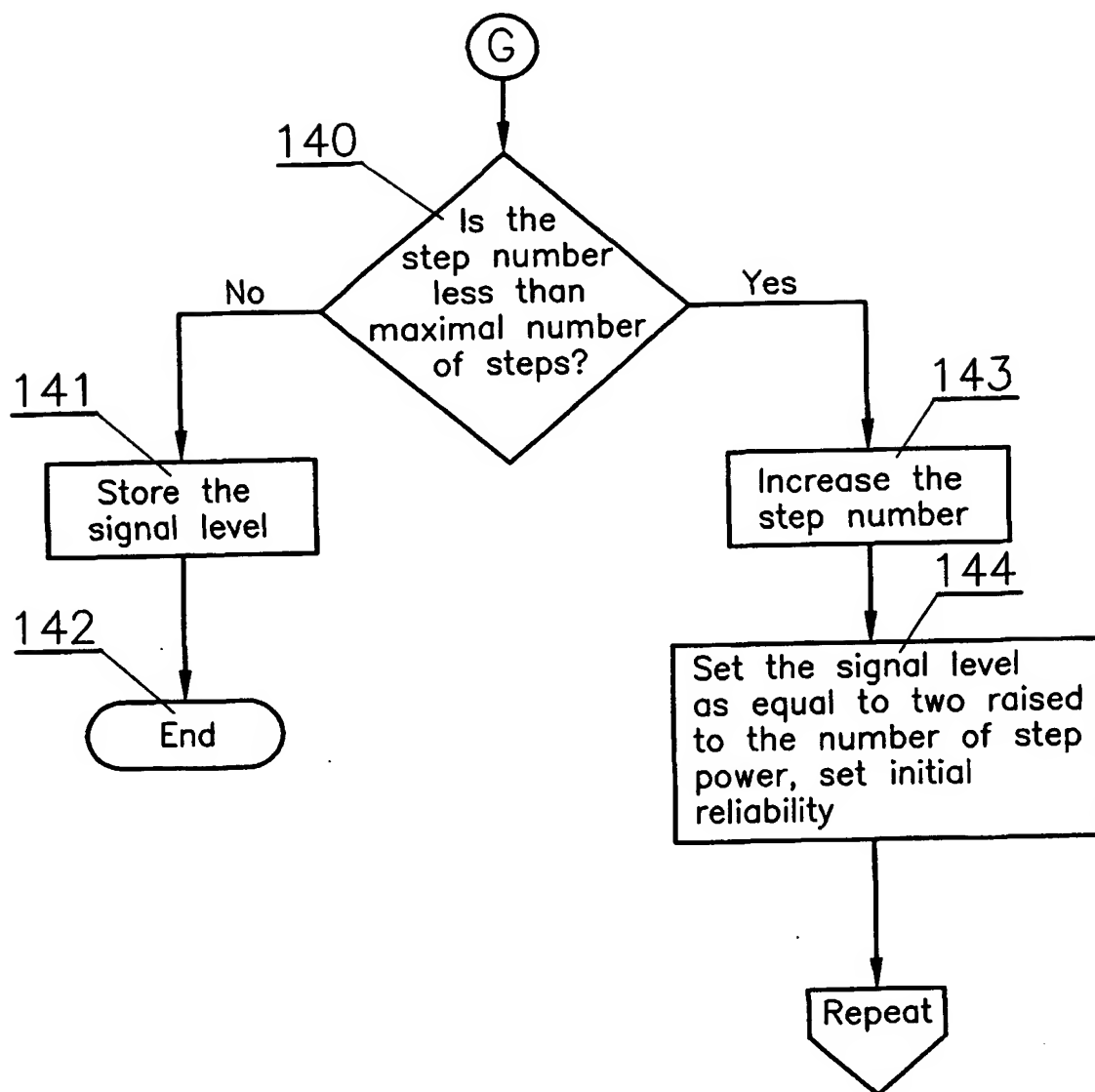


Fig.9C

17/23

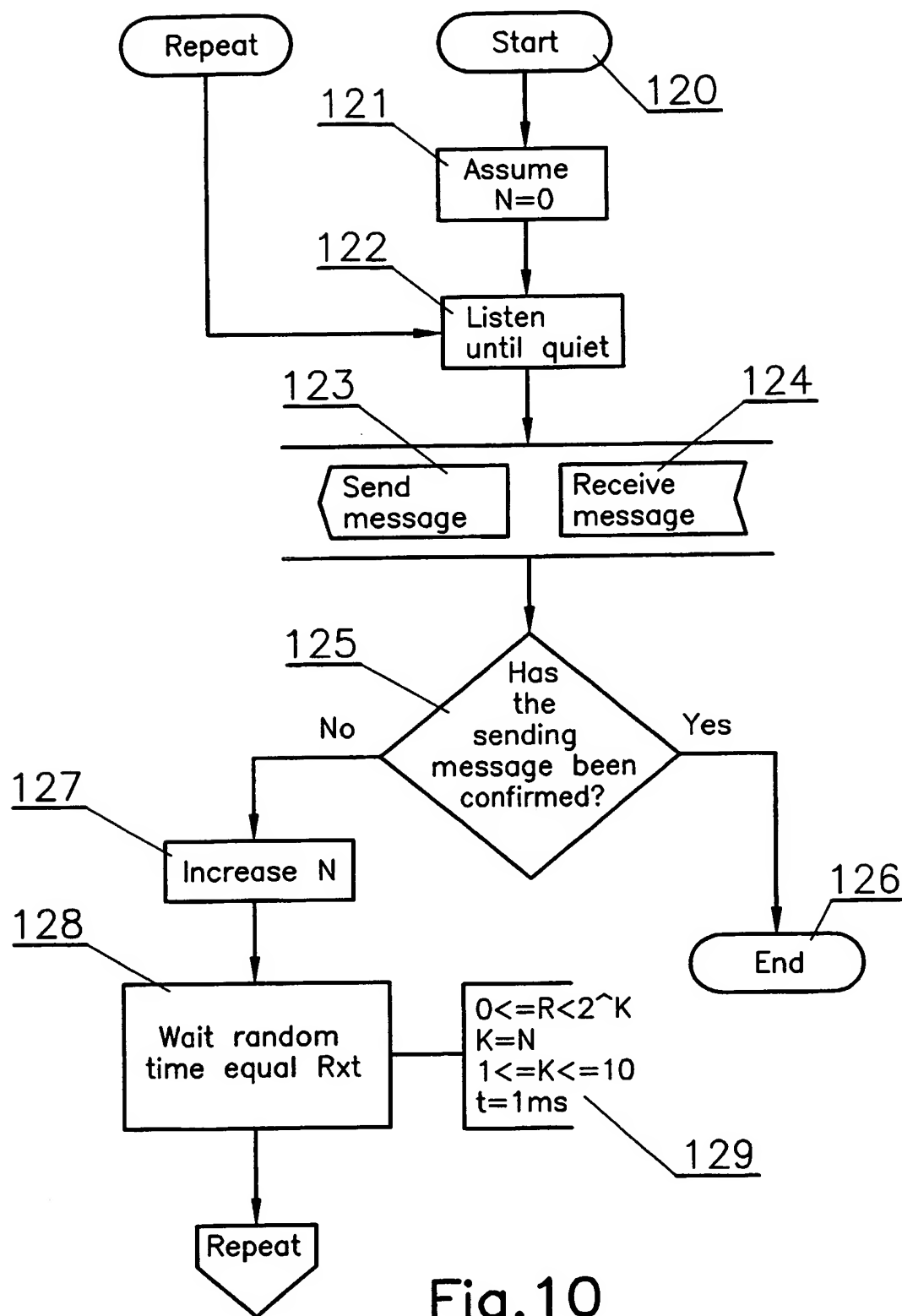


Fig.10

18/23

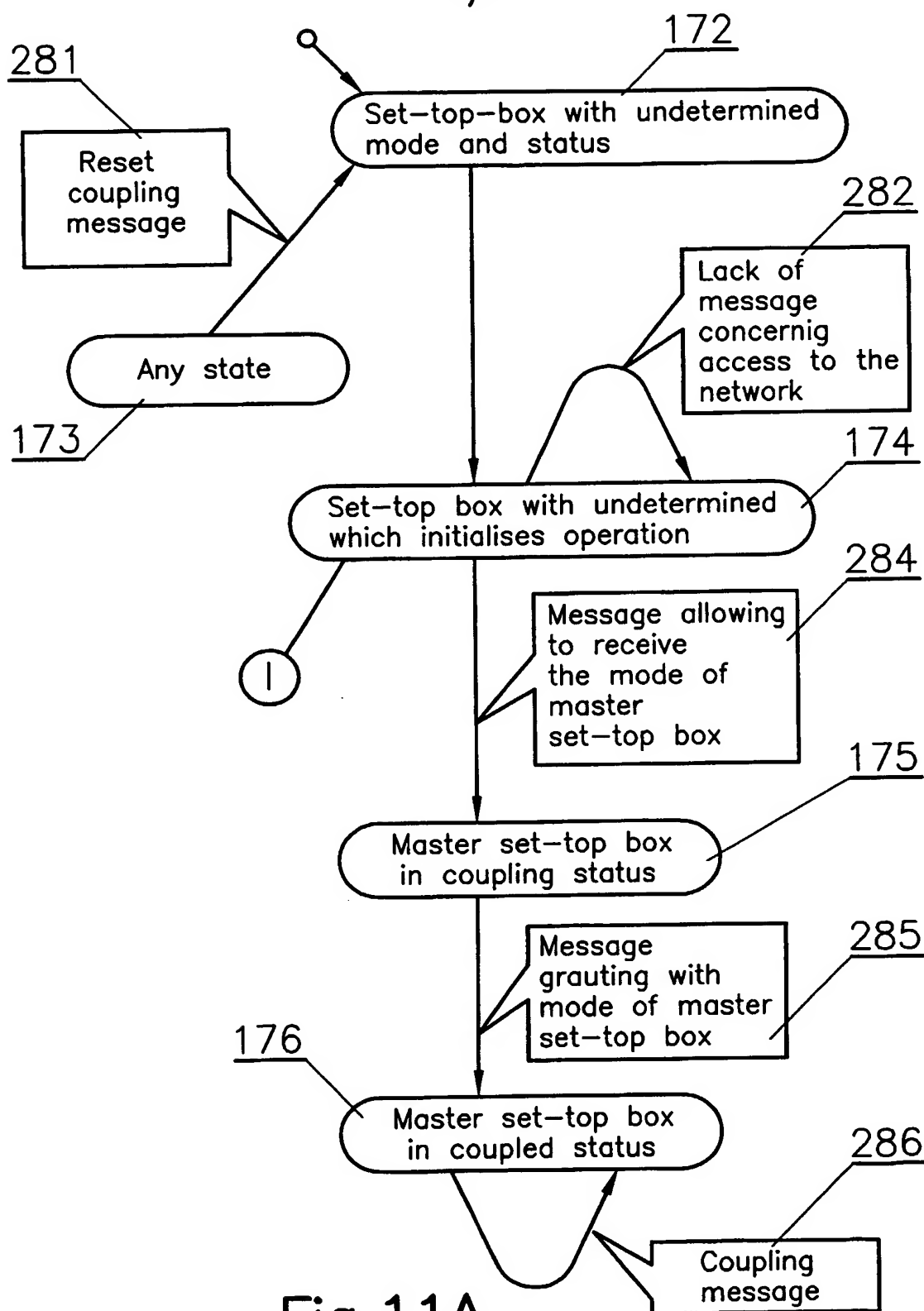


Fig.11A

19/23

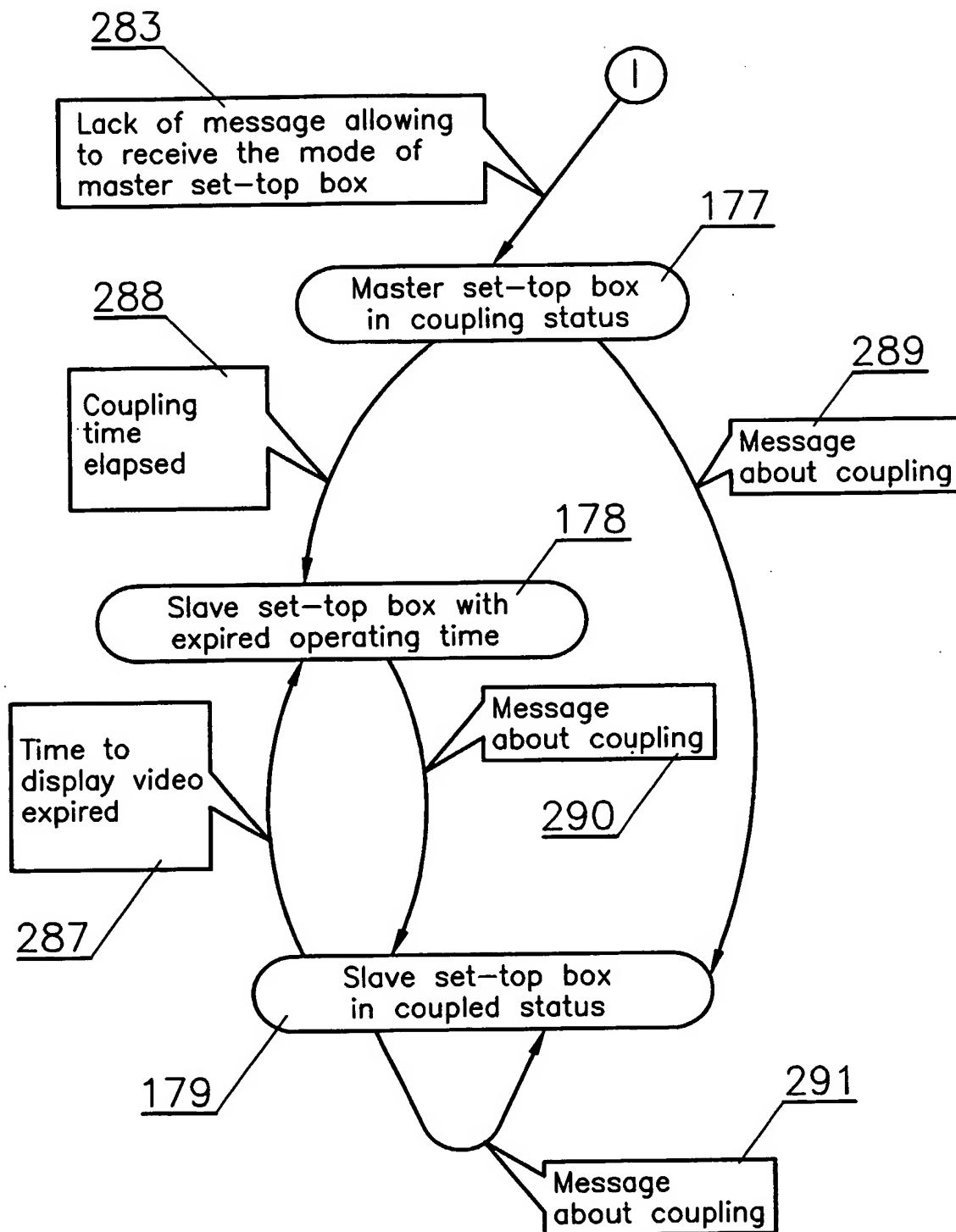


Fig.11B

20/23

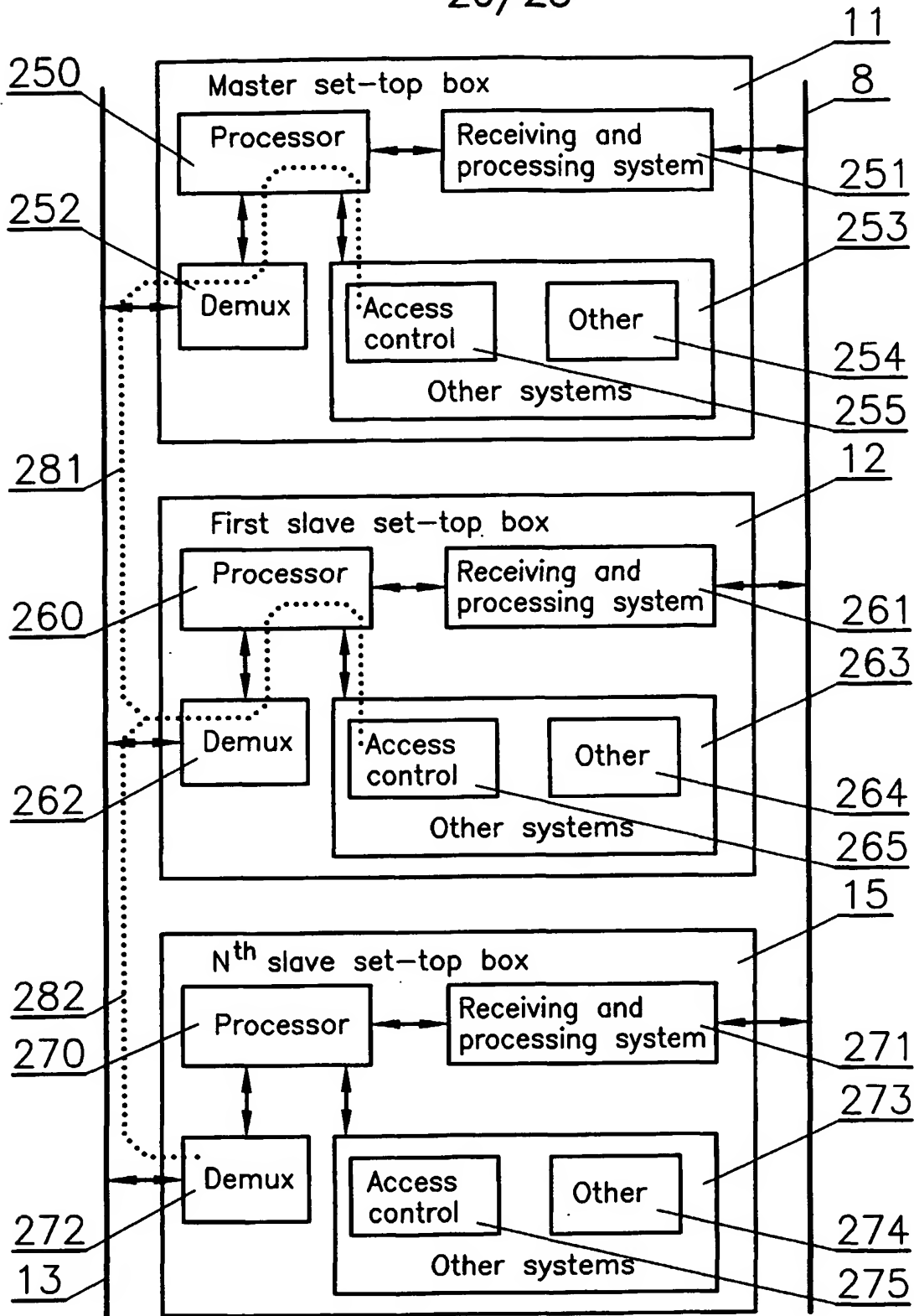


Fig.12

21/23

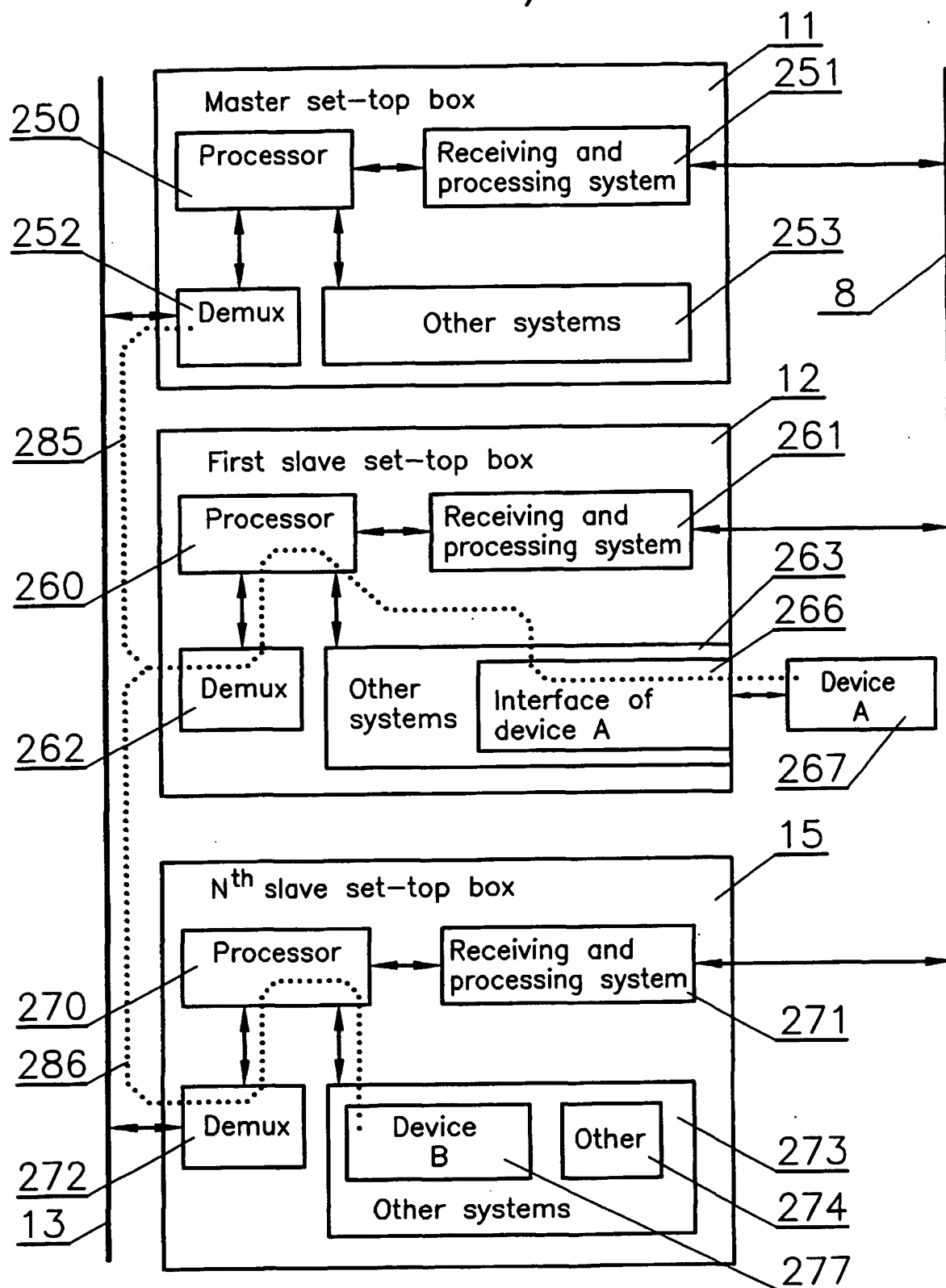


Fig.13

22/23

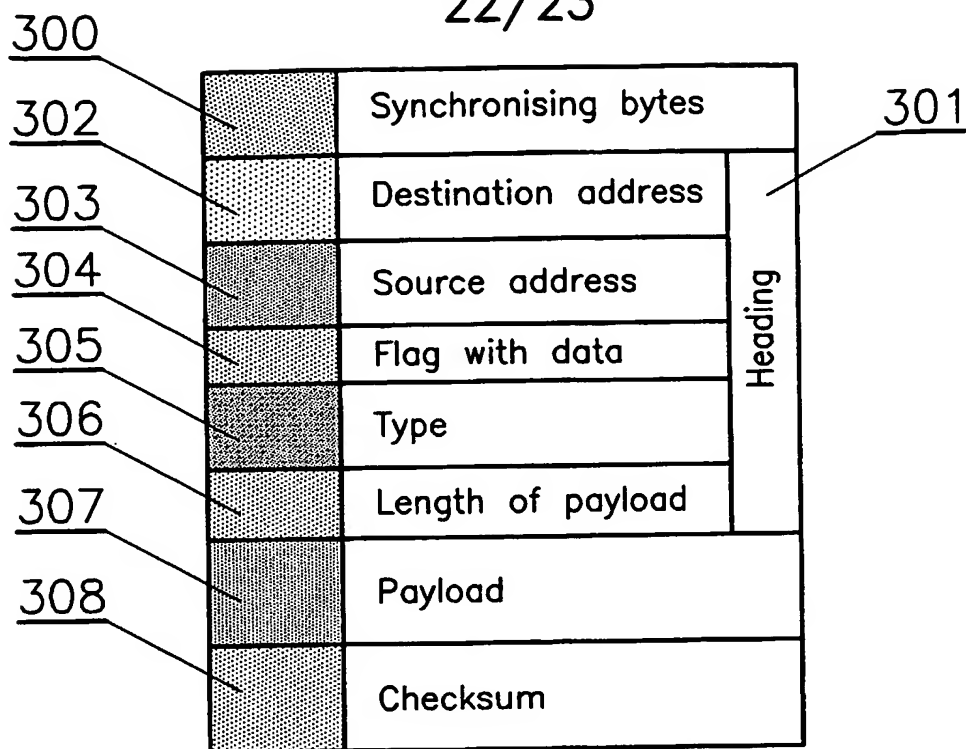


Fig.14

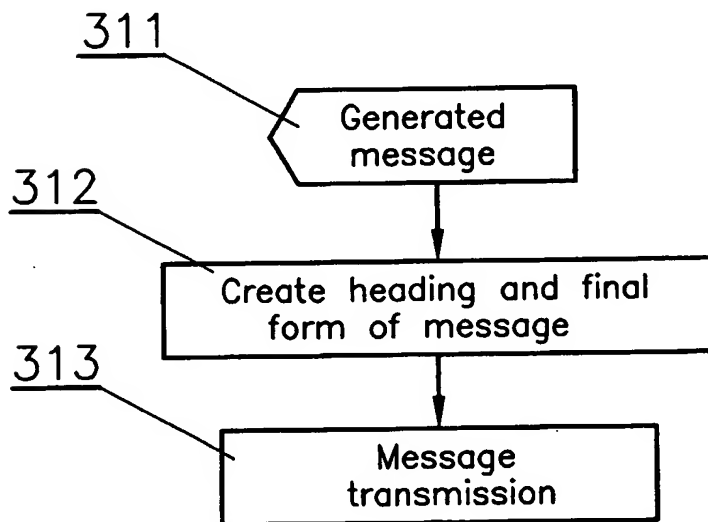


Fig.15

23/23

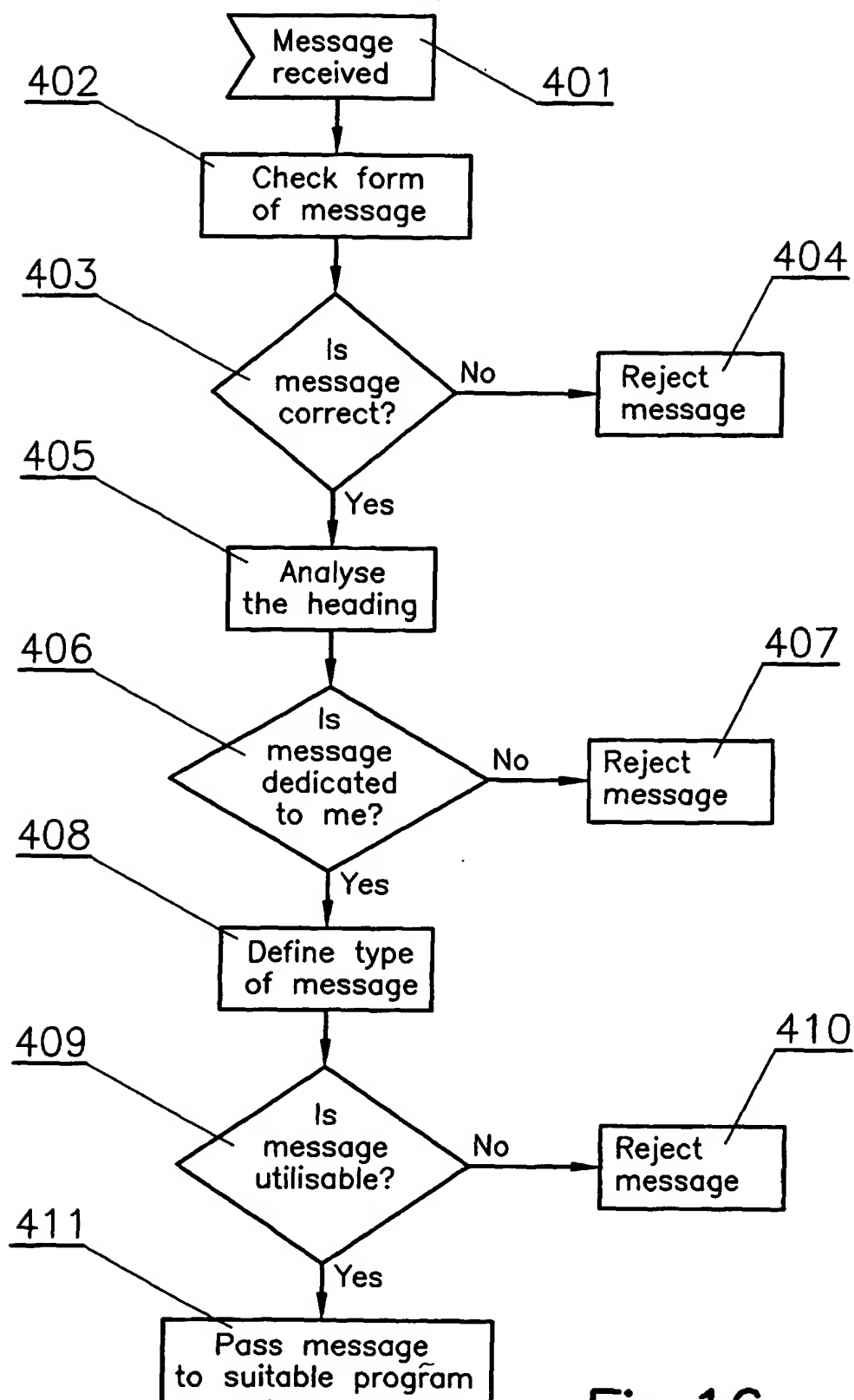


Fig.16

INTERNATIONAL SEARCH REPORT

International Application No

PCT/PL 03/00013

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EP0-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 04718 A (BENARDEAU CHRISTIAN ; CANAL PLUS SA (FR); DAUVOIS JEAN LUC (FR)) 27 January 2000 (2000-01-27) page 20, line 19 -page 28, line 5 figures 1-6 ---	1-7, 11-13, 25-29, 35-37
X	EP 0 726 676 A (PHILIPS ELECTRONICS NV ; PHILIPS ELECTRONICS NV (NL)) 14 August 1996 (1996-08-14) page 3, column 3, line 53 -page 4, column 6, line 10 figures 1-3 -----	1, 2, 25, 26



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

7 August 2003

Date of mailing of the international search report

14/08/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Van der Zaal, R

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/PL 03/00013

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0004718	A	27-01-2000	AT 226379 T	15-11-2002
			AU 755892 B2	02-01-2003
			AU 4642599 A	07-02-2000
			BR 9912091 A	03-04-2001
			CA 2337066 A1	27-01-2000
			CN 1317203 T	10-10-2001
			DE 69903557 D1	21-11-2002
			DE 69903557 T2	26-06-2003
			EP 1099348 A1	16-05-2001
			ES 2185365 T3	16-04-2003
			HR 20010033 A1	28-02-2002
			WO 0004718 A1	27-01-2000
			JP 2002521879 T	16-07-2002
			NO 20010227 A	15-03-2001
			NZ 509760 A	28-08-2002
			PL 345531 A1	17-12-2001
			TR 200100571 T2	23-07-2001
EP 0726676	A	14-08-1996	FR 2730372 A1	09-08-1996
			DE 69610343 D1	26-10-2000
			DE 69610343 T2	29-03-2001
			EP 0726676 A1	14-08-1996
			JP 8251569 A	27-09-1996
			US 5748732 A	05-05-1998